FIG.1

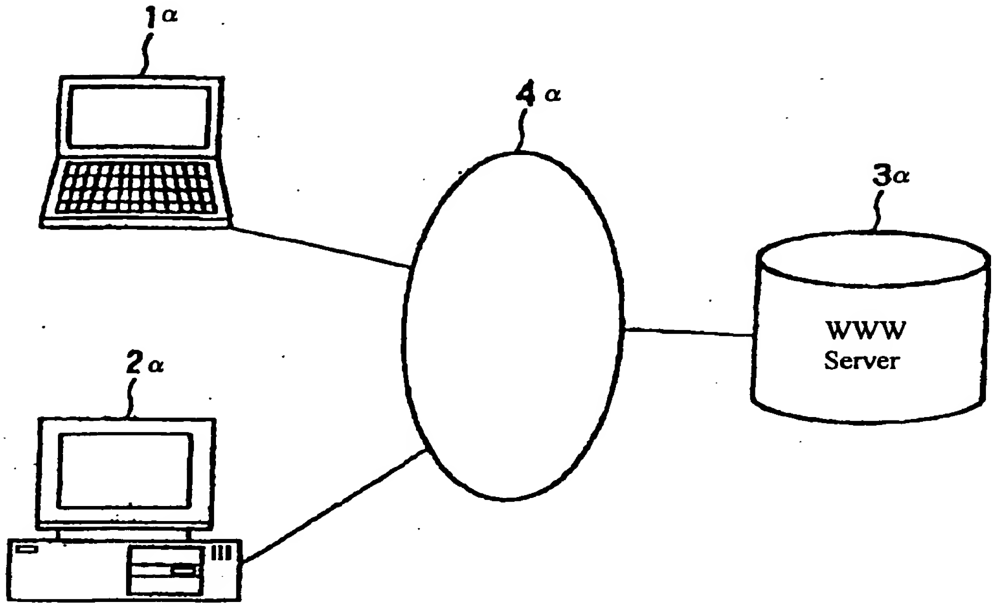


FIG.2

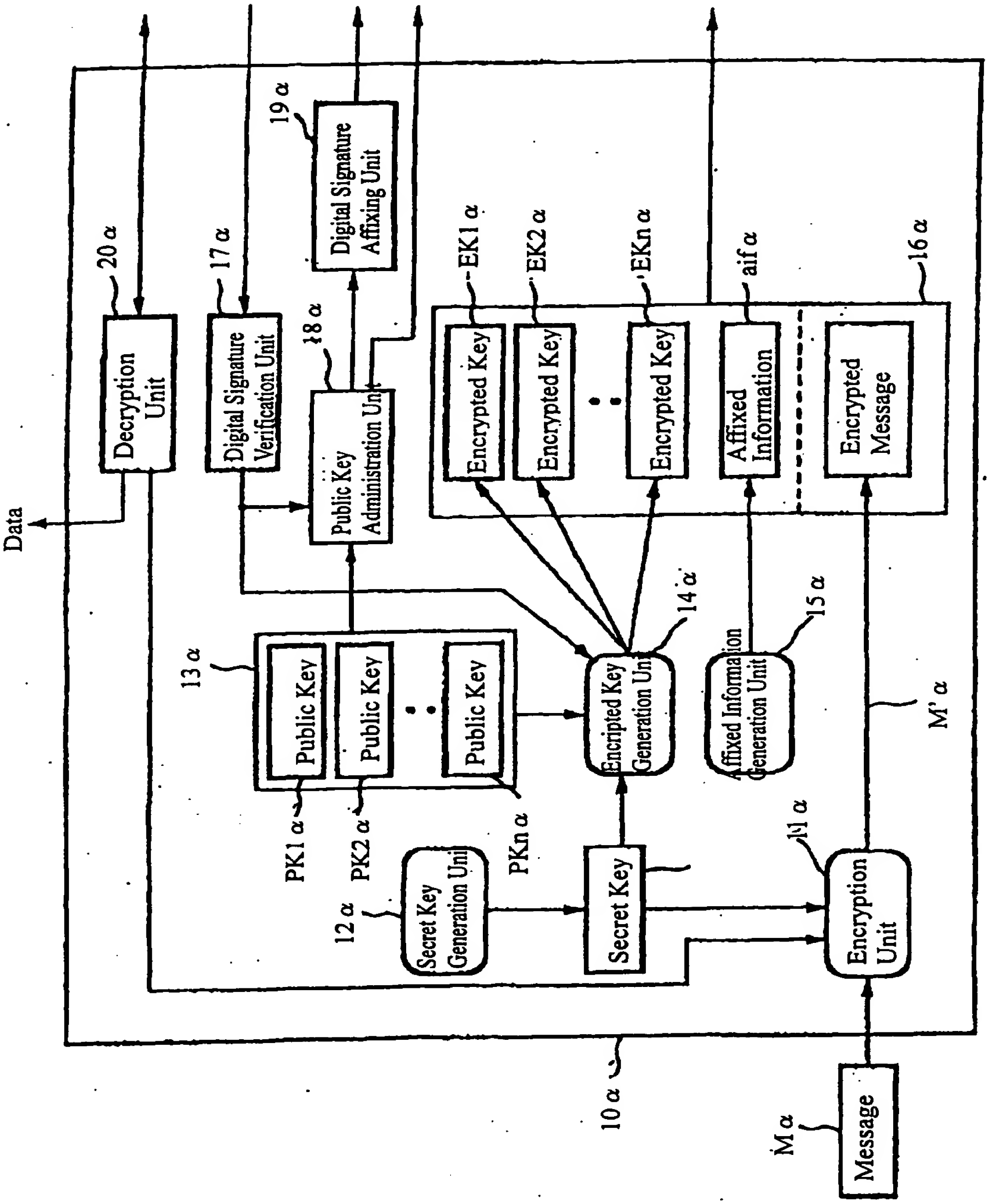

Data
20α
Decryption Unit
17α
Digital Signature Verification Unit
19α
Digital Signature Affixing Unit
18α
Public Key Administration Unit
EK1α
EK2α
EKnα
aifα
16α
Encrypted Key
Encrypted Key
Encrypted Key
Affixed Information
Encrypted Message
13α
Public Key
Public Key
Public Key
PK1α
PK2α
PKnα
14α
Encripted Key Generation Unit
15α
Affixed Information Generation Unit
M'α
12α
Secret Key Generation Unit
Secret Key
11α
Encryption Unit
10α
Mα
Message

FIG.3

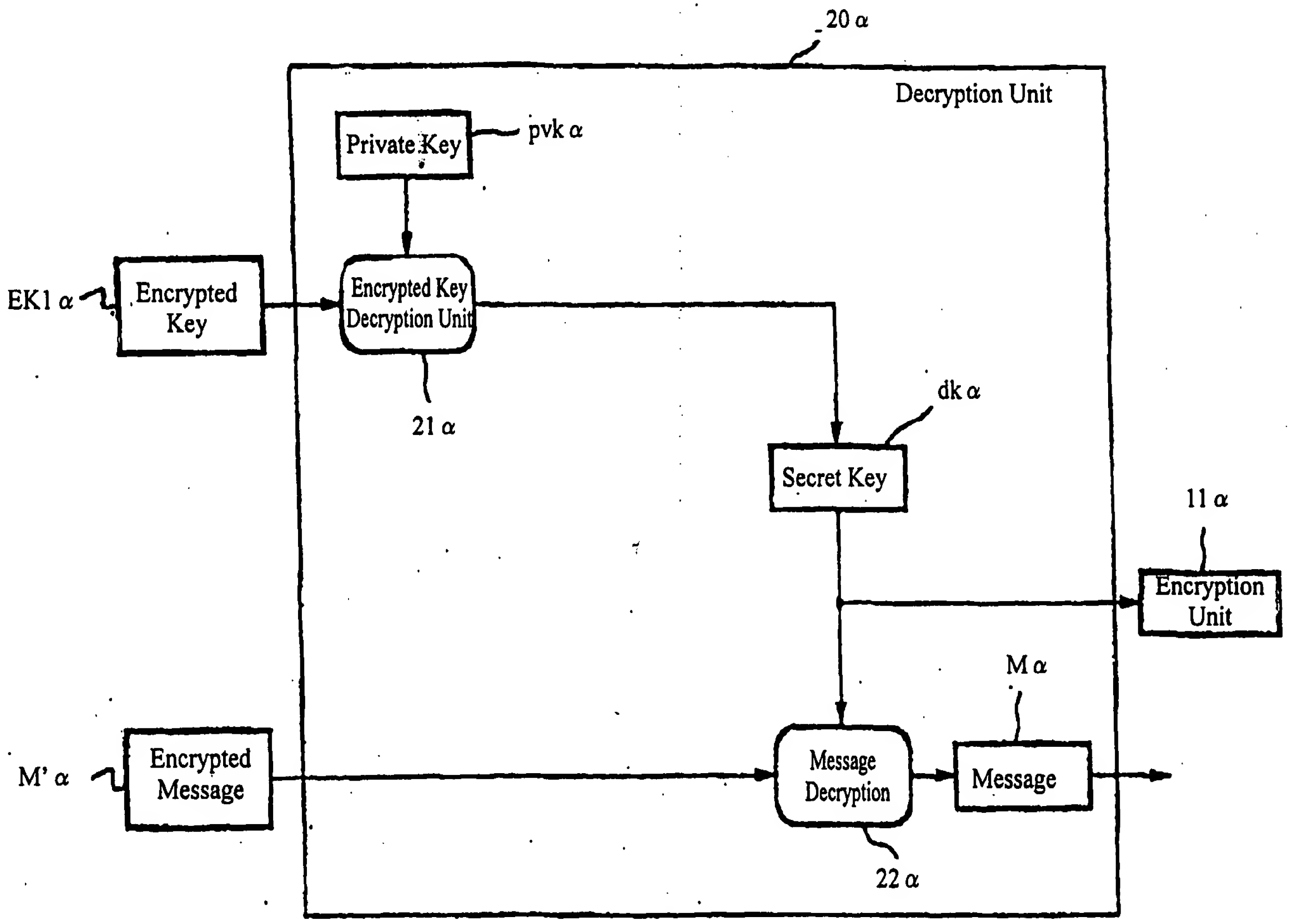

20 α
Decryption Unit
Private Key
pvk α
EK1 α
Encrypted Key
Encrypted Key Decryption Unit
21 α
dk α
Secret Key
11 α
Encryption Unit
M α
M' α
Encrypted Message
Message Decryption
Message
22 α

FIG.4

DBMS

Permission Test Unit

Member List GL α

Group ID	Public Key Serial No.	Member Public Key
:	:	:

Team Member's Digital Signature

Secret Key List CKL α

Secret Key No.	Public Key Serial No.	Encrypted Key
122	11 : AA	qwer
122	1C : FF	zxcv
122	E5 : 4B	wurt

Group Secret Key List G CKL α

Group ID	Secret Key No.
B team	123

Encrypted Data List EDL α

Data ID	Encrypted Data
4444	iiiiiiiiiiiiiiii

Data & Secret Key List DCKL α

Data ID	Secret Key No.
4444	123

FIG.5

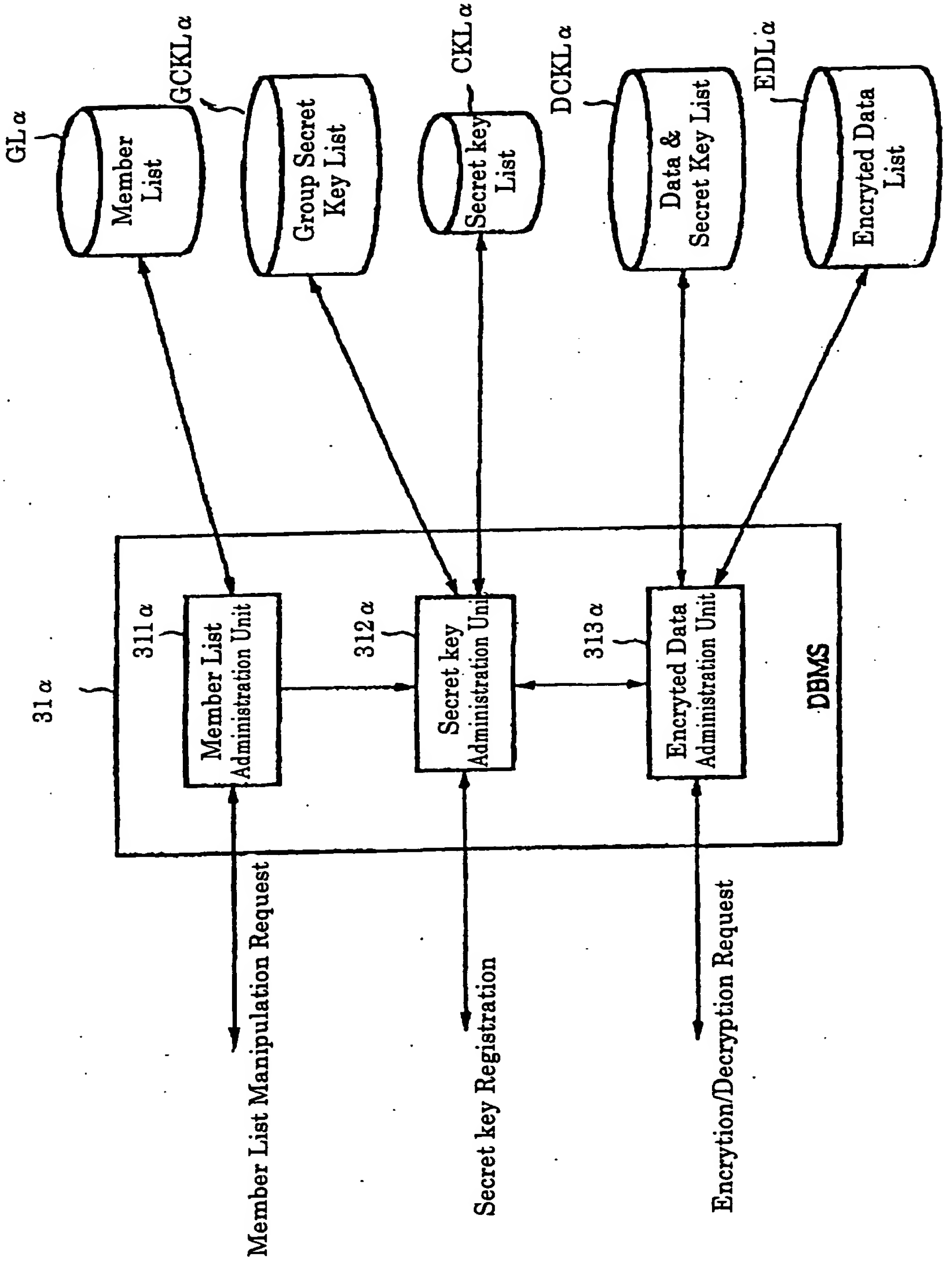
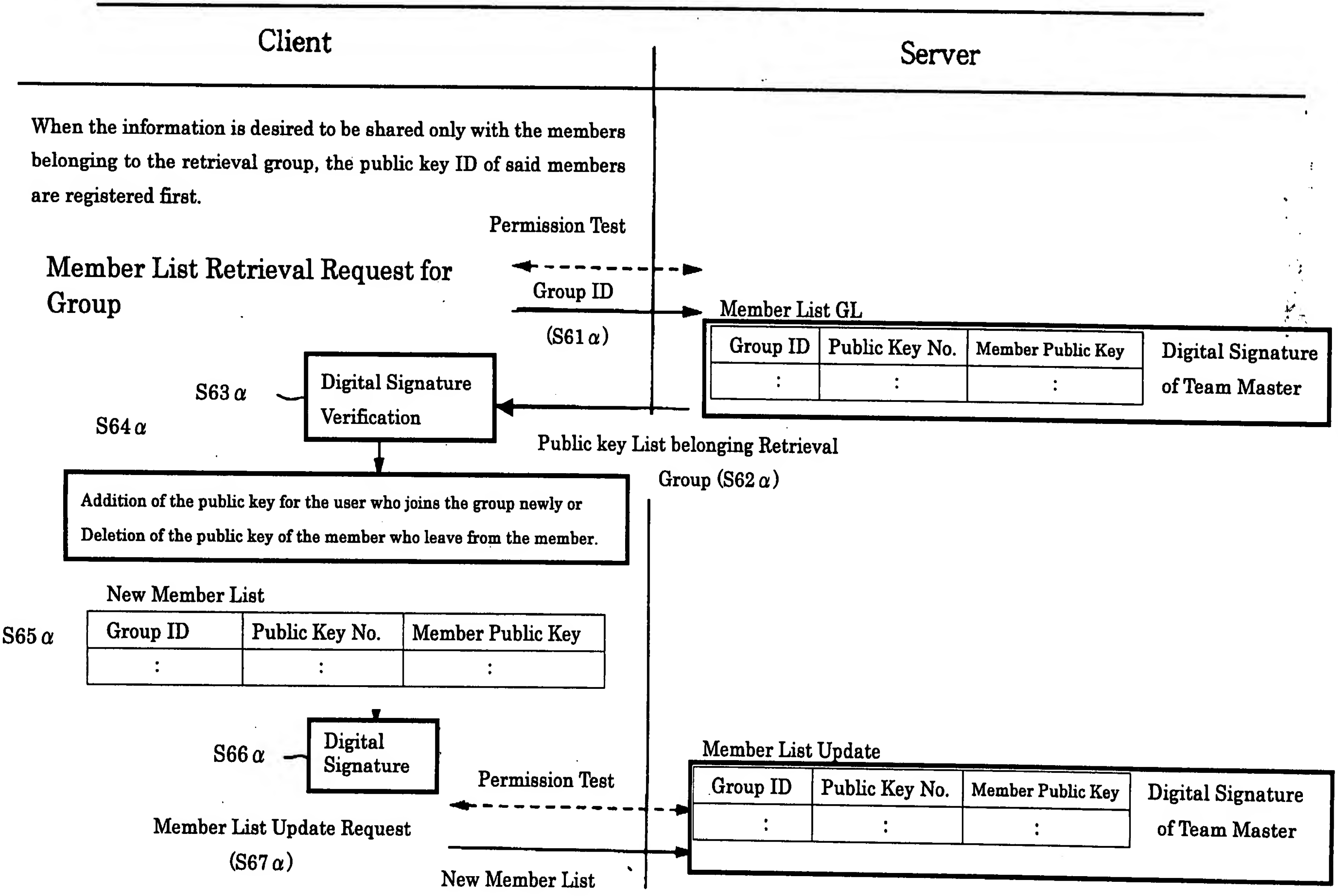

31α
311α
Member List Administration Unit
312α
Secret key Administration Unit
313α
Encryted Data Administration Unit
DBMS
GLα
Member List
GCKLα
Group Secret Key List
CKLα
Secret key List
DCKLα
Data & Secret Key List
EDLα
Encryted Data List
Member List Manipulation Request
Secret key Registration
Encrytion/Decryption Request

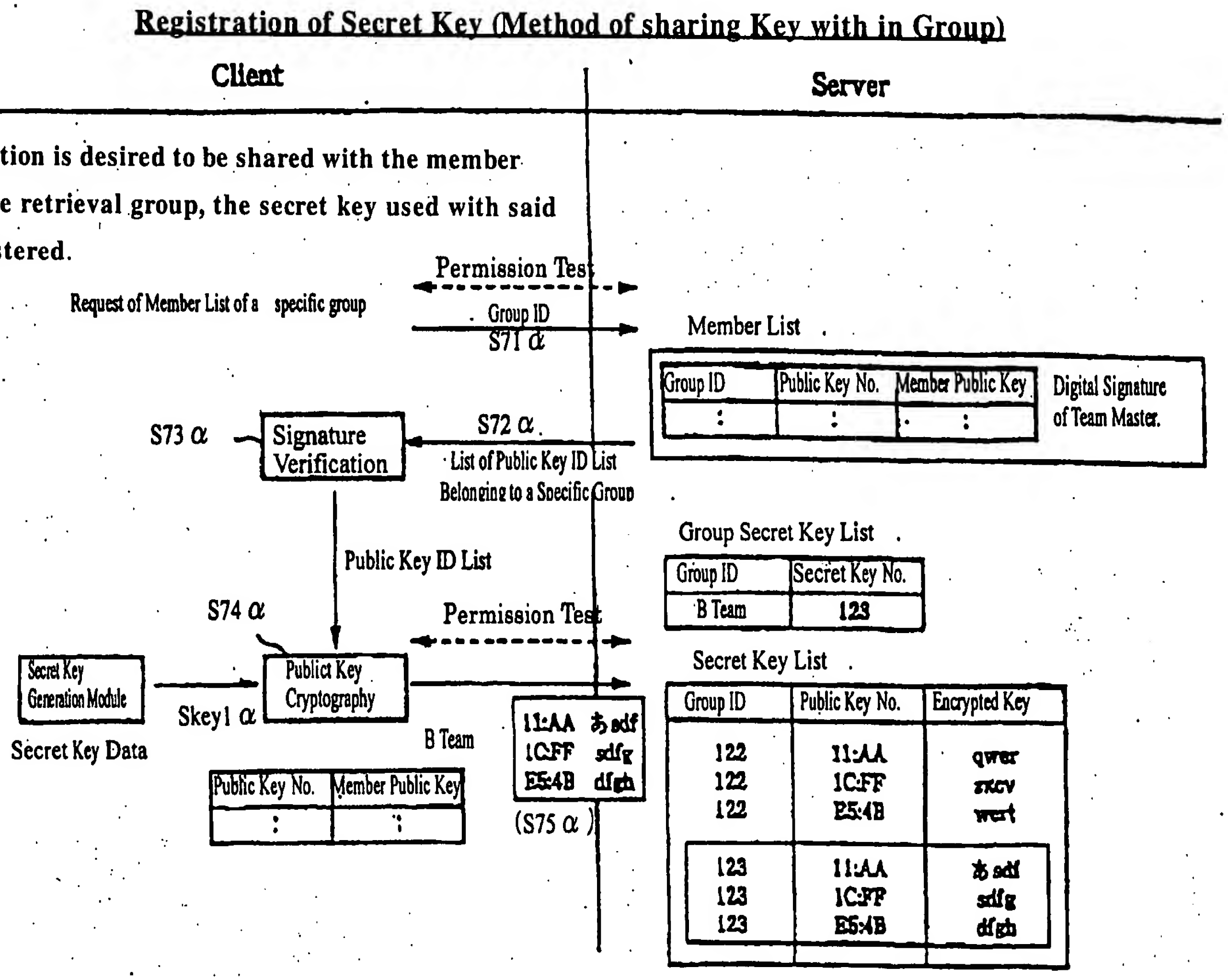
FIG.6 Example : Registration of Public key ID for Group (Method of sharing secret key within the group)



When the information is desired to be shared only with the members belonging to the retrieval group, the public key ID of said members are registered first.

Addition of the public key for the user who joins the group newly or Deletion of the public key of the member who leave from the member.

FIG.7



When the information is desired to be shared with the member Belonging with the retrieval group, the secret key used with said members are registered.

OBLON ET AL (703) 413-3000
DOCKET # 199691US2PCT SHEET 7 OF 73

09/700390

FIG.8

Example of Encryption (Method of Sharing Secret Key within Group)

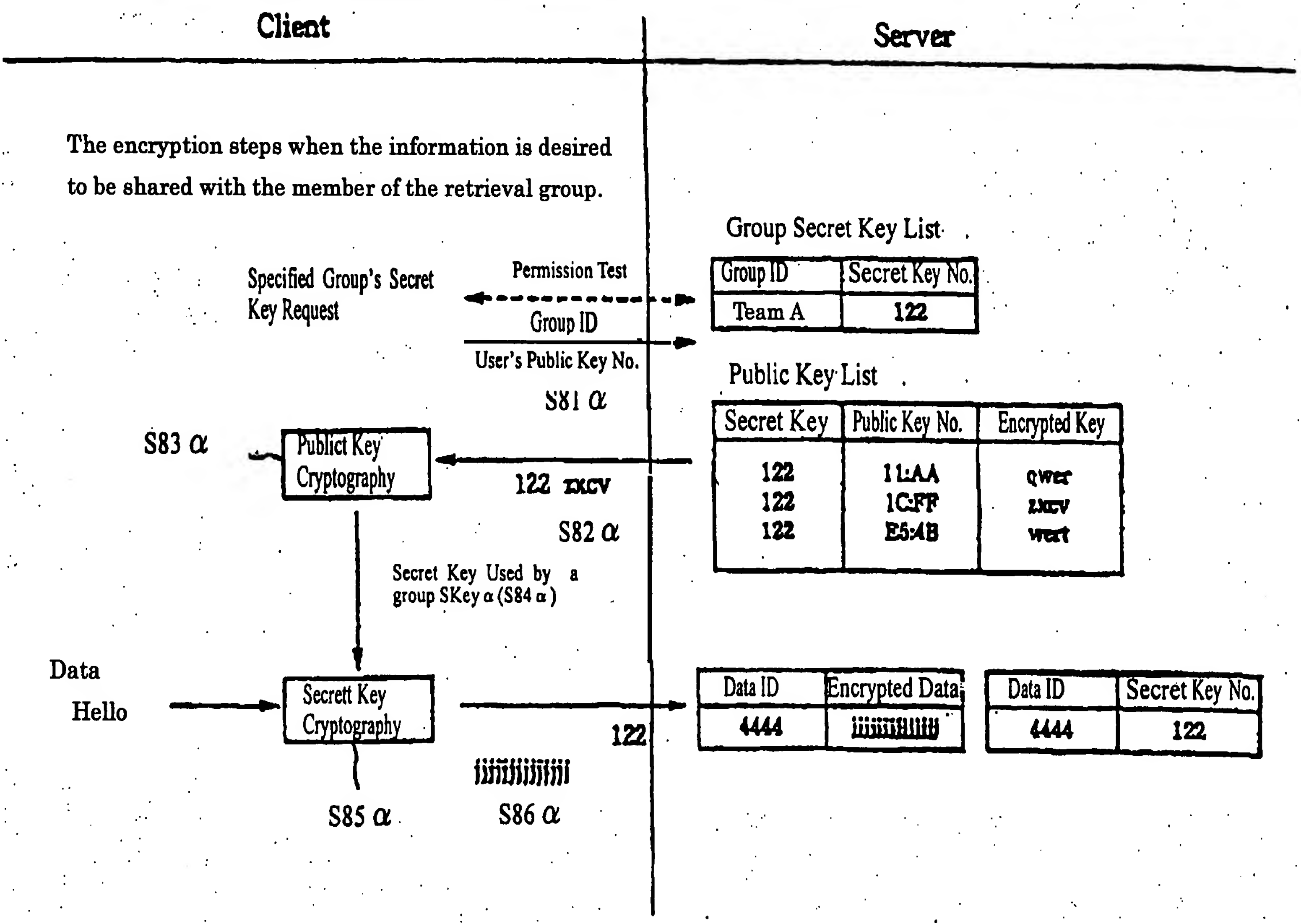
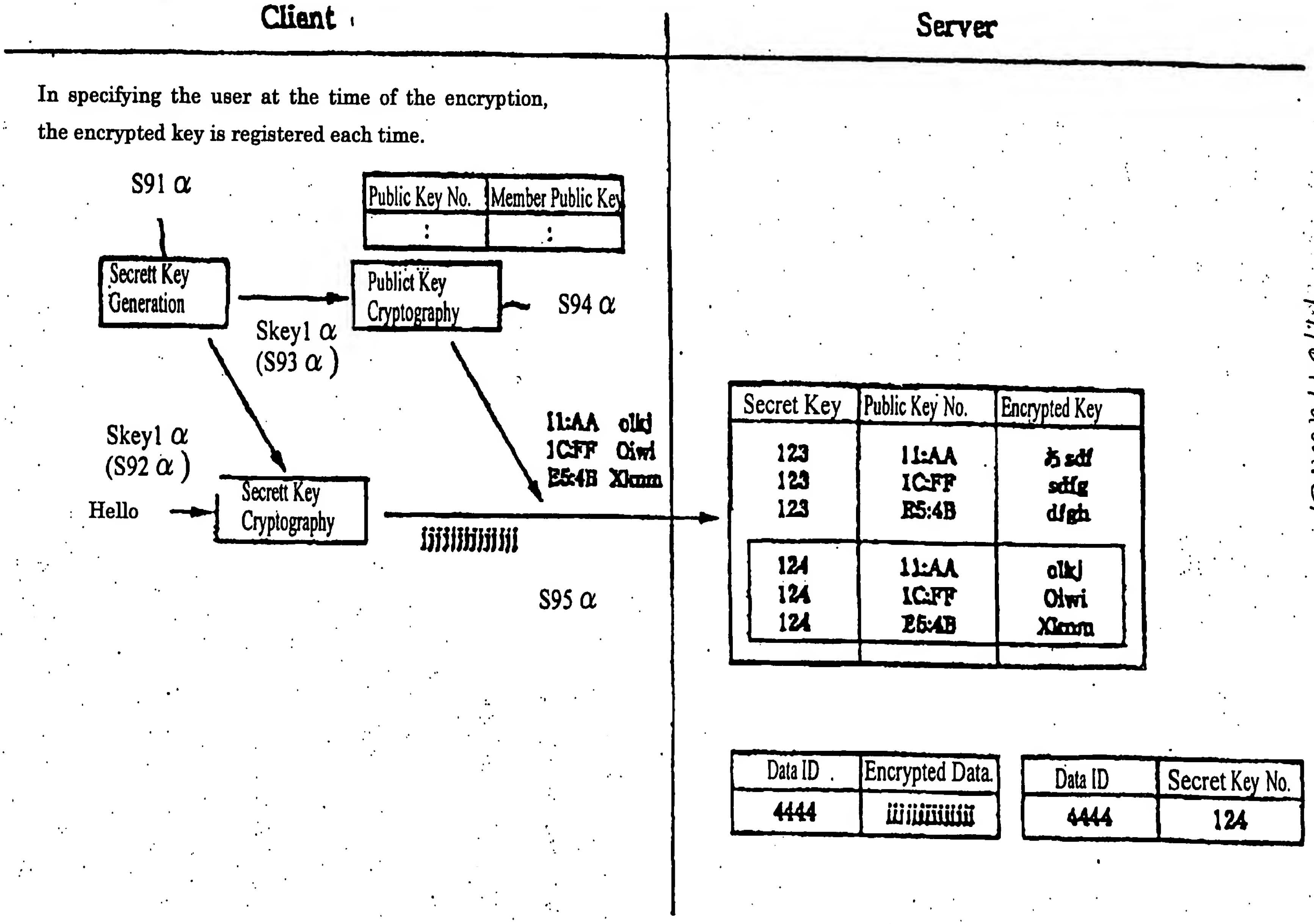


FIG. 9 Example of Encryption (Method of Sharing Secret Key with respectively selected user)



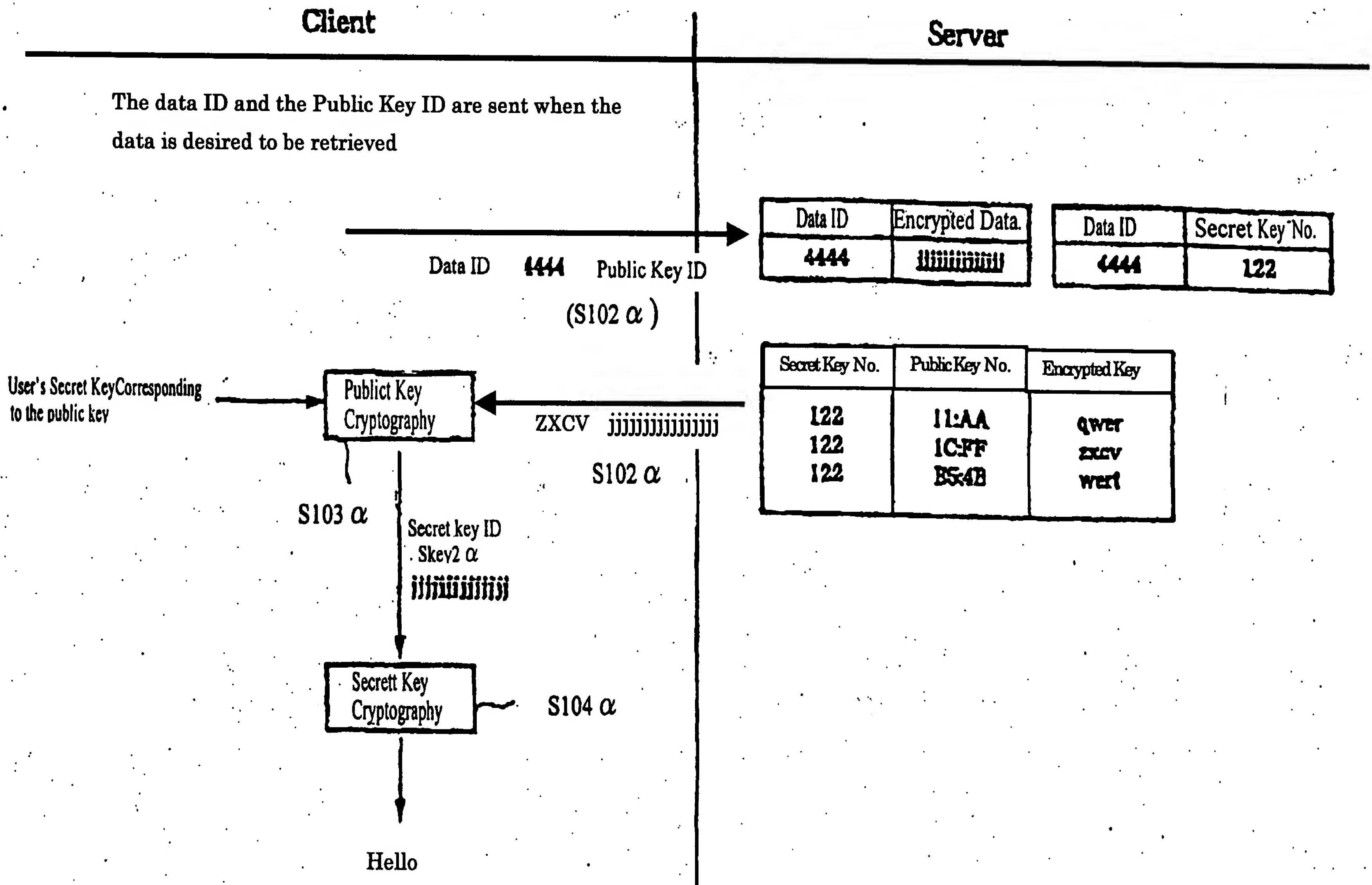
In specifying the user at the time of the encryption, the encrypted key is registered each time.

09/700390

OBLON ET AL (703) 413-3000
DOCKET # 199691US2PCT SHEET 10 OF 73

FIG.10

Example of Decryption (Both Case)



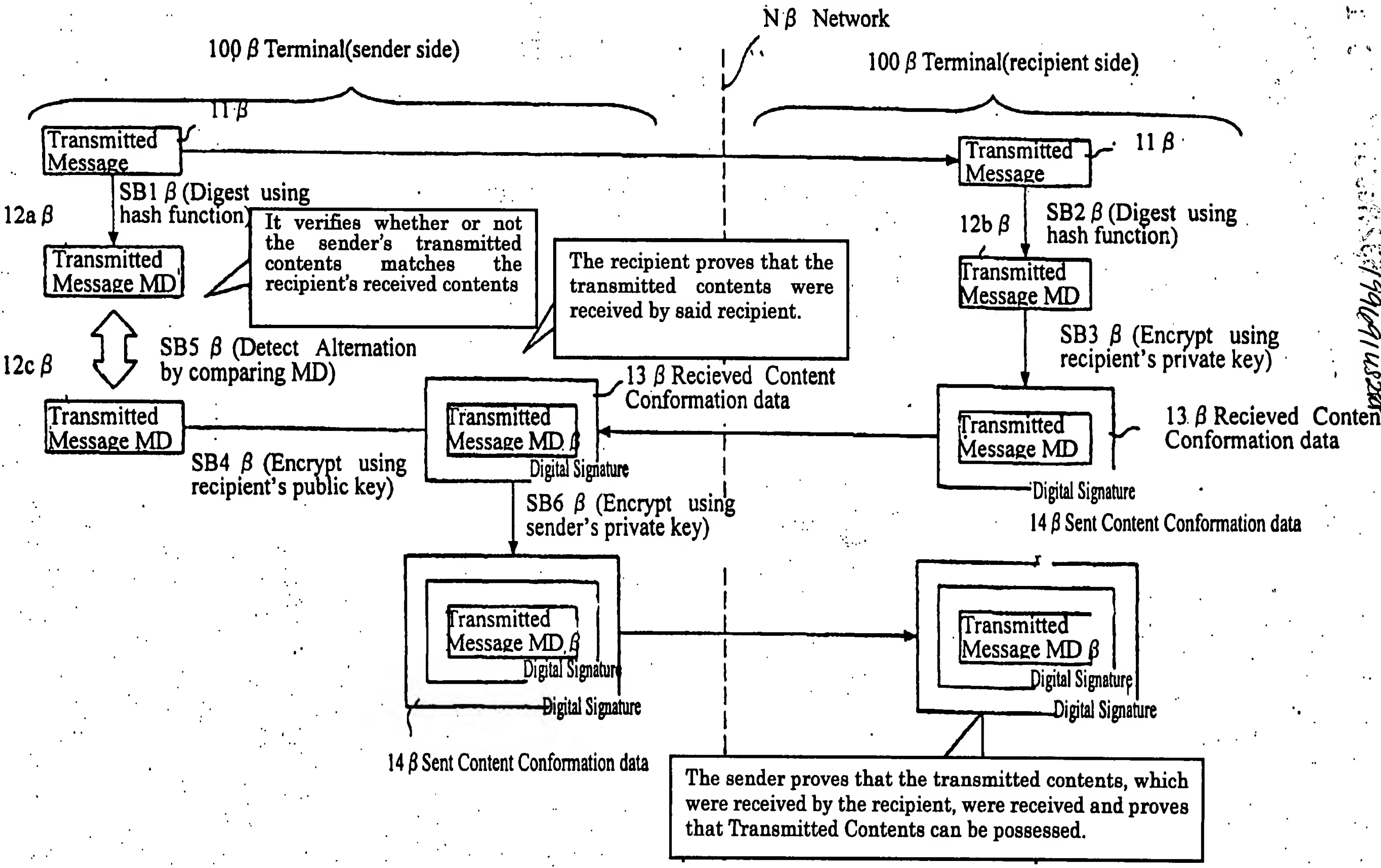
Client
Server
The data ID and the Public Key ID are sent when the data is desired to be retrieved
Data ID 4444 Public Key ID
(S102 α)
User's Secret KeyCorresponding to the public key
Publict Key Cryptography
ZXCV jjjjjjjjjjjjjjj
S102 α
S103 α
Secret key ID
Skey2 α
jjjjjjjjjjjjj
Secrett Key Cryptography
S104 α
Hello

Data ID	Encrypted Data.
4444	jjjjjjjjjjjjj

Data ID	Secret Key No.
4444	122

Secret Key No.	Public Key No.	Encrypted Key
122 122 122	11:AA 1C:FF B5:4B	qwer zxcv wert

FIG11


Nβ Network
100β Terminal(sender side)
100β Terminal(recipient side)
11β
Transmitted Message
SB1β (Digest using hash function)
12aβ
Transmitted Message MD
SB5β (Detect Alternation by comparing MD)
12cβ
Transmitted Message MD
SB4β (Encrypt using recipient's public key)
13β Recieved Content Conformation data
Transmitted Message MDβ
Digital Signature
SB6β (Encrypt using sender's private key)
Transmitted Message MDβ
Digital Signature
Digital Signature
14β Sent Content Conformation data
11β
Transmitted Message
SB2β (Digest using hash function)
12bβ
Transmitted Message MD
SB3β (Encrypt using recipient's private key)
Transmitted Message MD
Digital Signature
13β Recieved Content Conformation data
14β Sent Content Conformation data
Transmitted Message MDβ
Digital Signature
Digital Signature

It verifies whether or not the sender's transmitted contents matches the recipient's received contents

The recipient proves that the transmitted contents were received by said recipient.

The sender proves that the transmitted contents, which were received by the recipient, were received and proves that Transmitted Contents can be possessed.

FIG12

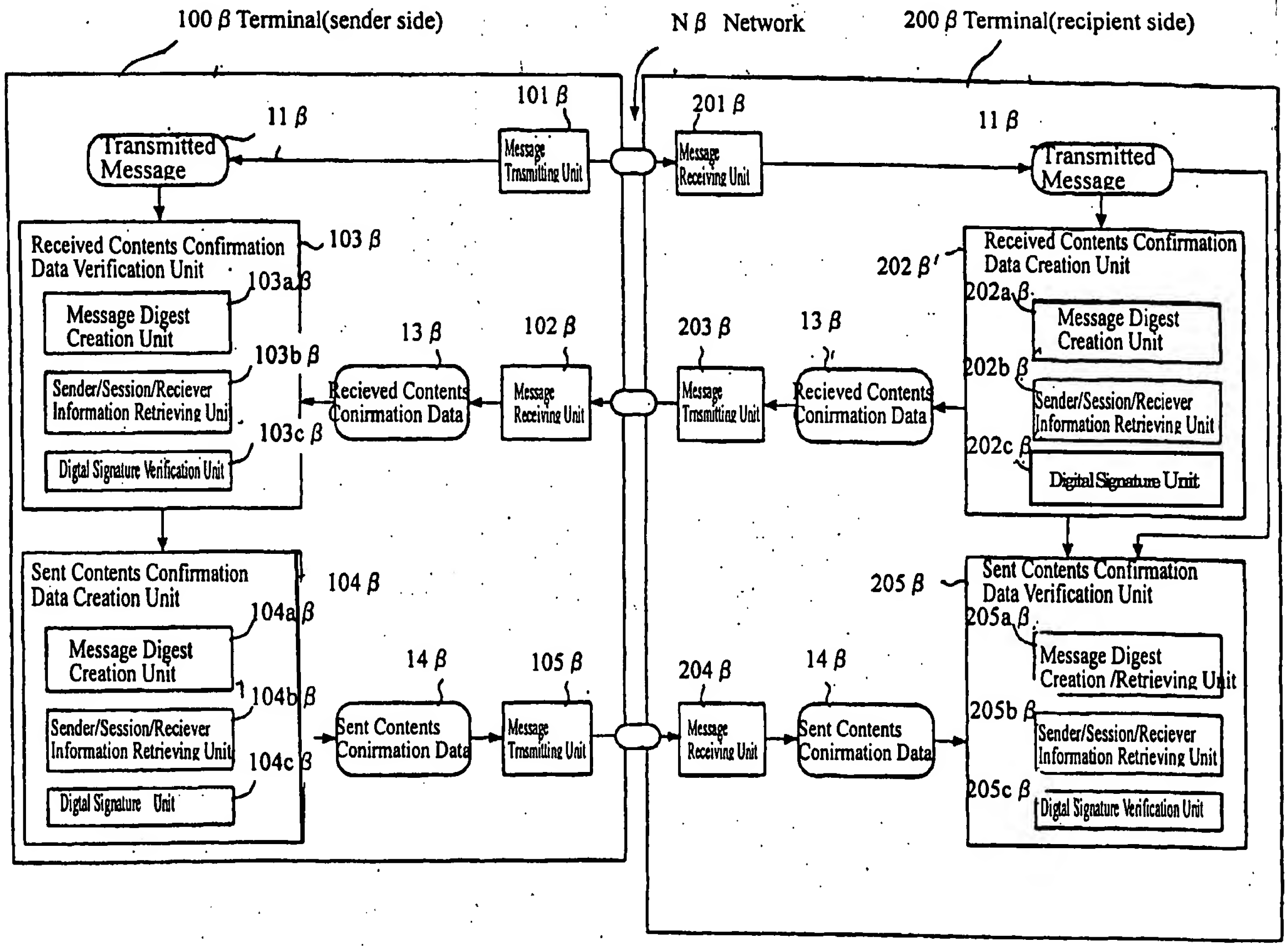

100 β Terminal(sender side)
N β Network
200 β Terminal(recipient side)
11 β
Transmitted Message
101 β
Message Trsmitting Unit
201 β
Message Receiving Unit
11 β
Transmitted Message
Received Contents Confirmation Data Verification Unit
103 β
103a β
Message Digest Creation Unit
103b β
Sender/Session/Reciever Information Retrieving Uni
103c β
Digtal Signature Verification Unit
13 β
Recieved Contents Conirmation Data
102 β
Message Receiving Unit
203 β
Message Trsmitting Unit
13 β
Recieved Contents Conirmation Data
202 β'
Received Contents Confirmation Data Creation Unit
202a β
Message Digest Creation Unit
202b β
Sender/Session/Reciever Information Retrieving Unit
202c β
Digital Signature Unit
Sent Contents Confirmation Data Creation Unit
104 β
104a β
Message Digest Creation Unit
104b β
Sender/Session/Reciever Information Retrieving Unit
104c β
Digtal Signature Unit
14 β
Sent Contents Conirmation Data
105 β
Message Trsmitting Unit
204 β
Message Receiving Unit
14 β
Sent Contents Conirmation Data
205 β
Sent Contents Confirmation Data Verification Unit
205a β
Message Digest Creation /Retrieving Unit
205b β
Sender/Session/Reciever Information Retrieving Unit
205c β
Digtal Signature Verification Unit

FIG13

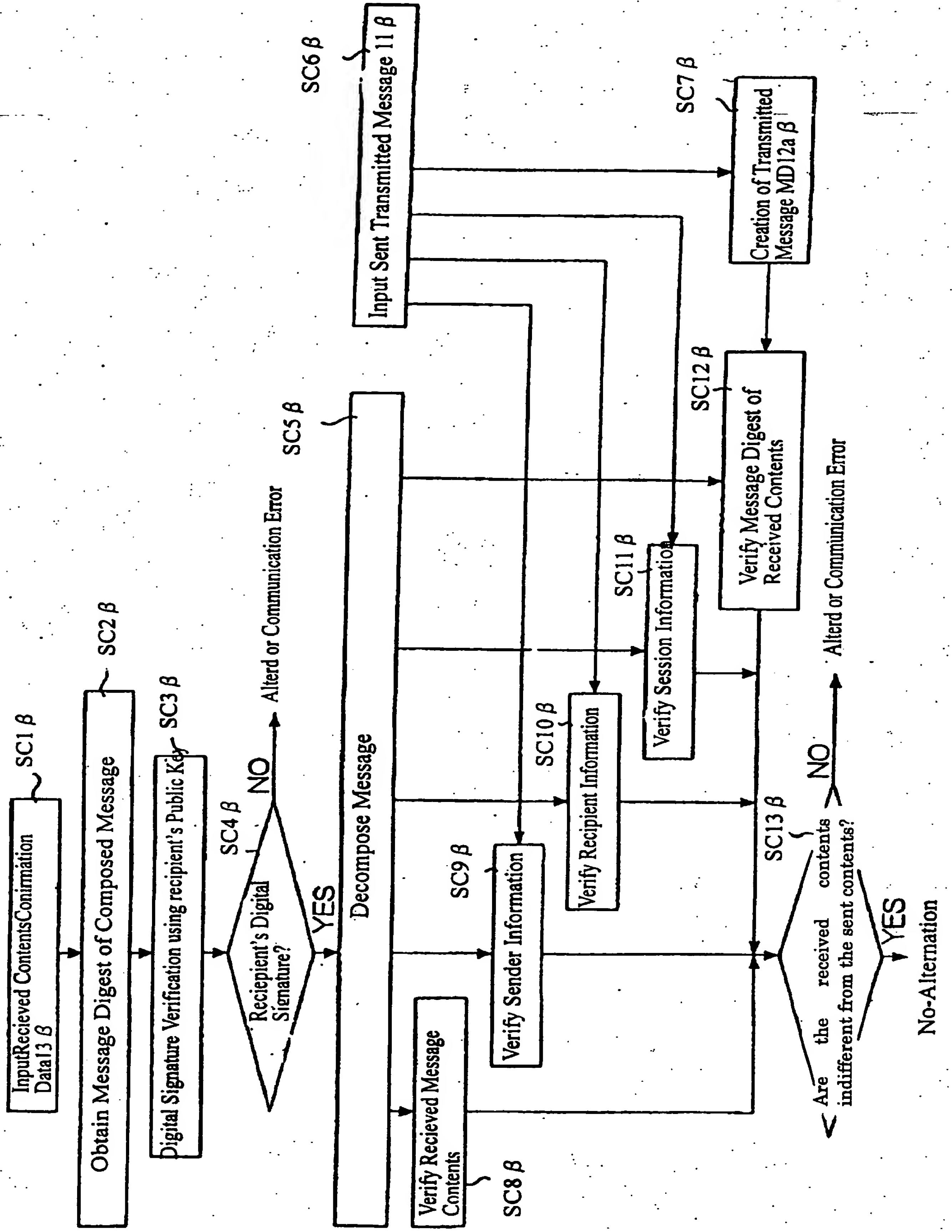

SC1 β
InputRecieved ContentsConirmation Data13 β
SC2 β
Obtain Message Digest of Composed Message
SC3 β
Digital Signature Verification using recipient's Public Key
SC4 β
Reciepient's Digital Signature?
NO
Alterd or Communication Error
YES
SC5 β
Decompose Message
SC6 β
Input Sent Transmitted Message 11 β
SC7 β
Creation of Transmitted Message MD12a β
SC8 β
Verify Recieved Message Contents
SC9 β
Verify Sender Information
SC10 β
Verify Recipient Information
SC11 β
Verify Session Information
SC12 β
Verify Message Digest of Received Contents
SC13 β
Are the received contents indifferent from the sent contents?
NO
Alterd or Communication Error
YES
No-Alternation

FIG14

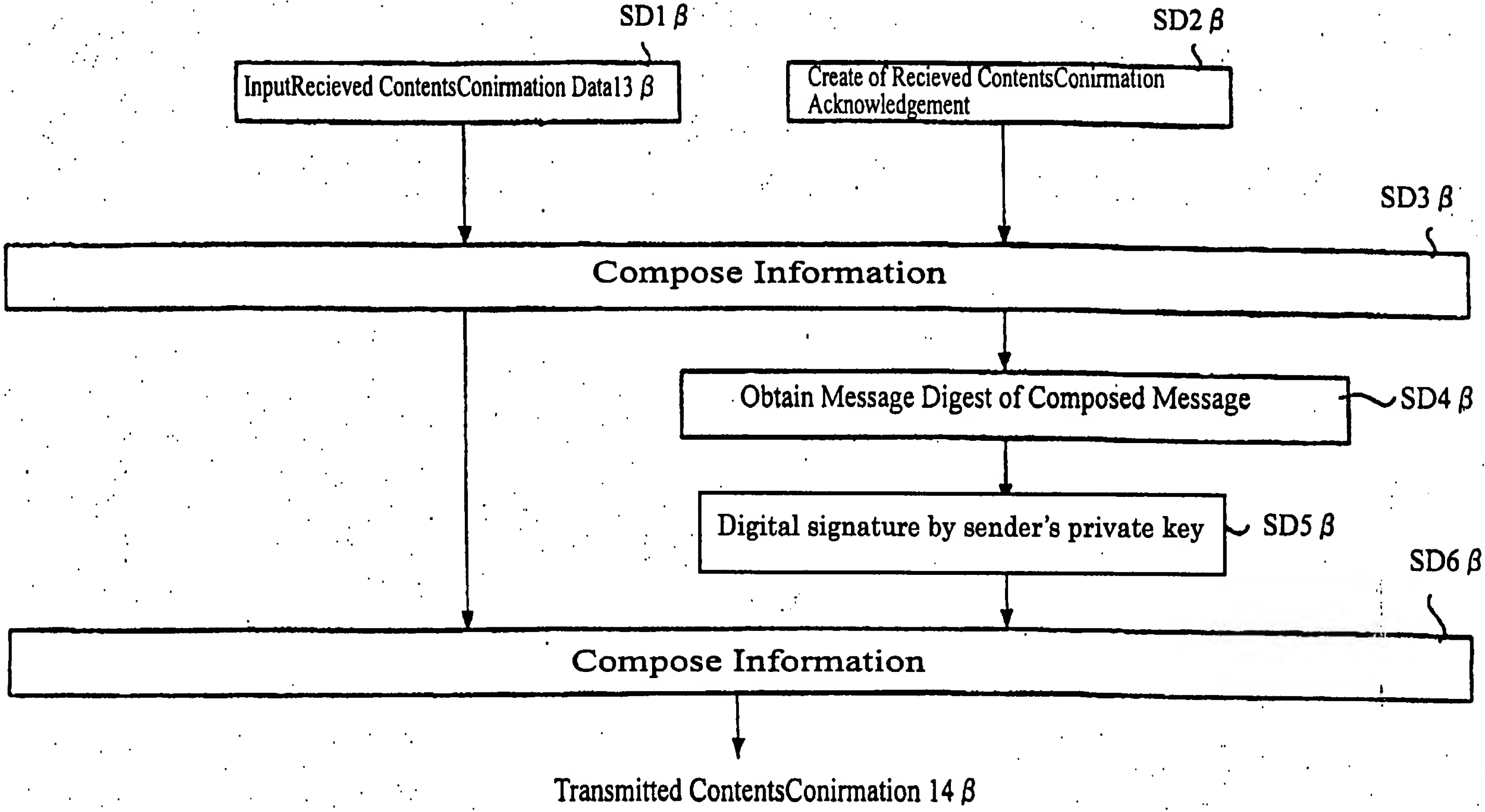

SD1 β
InputRecieved ContentsConirmation Data13 β
SD2 β
Create of Recieved ContentsConirmation Acknowledgement
SD3 β
Compose Information
Obtain Message Digest of Composed Message
SD4 β
Digital signature by sender's private key
SD5 β
SD6 β
Compose Information
Transmitted ContentsConirmation 14 β

FIG15

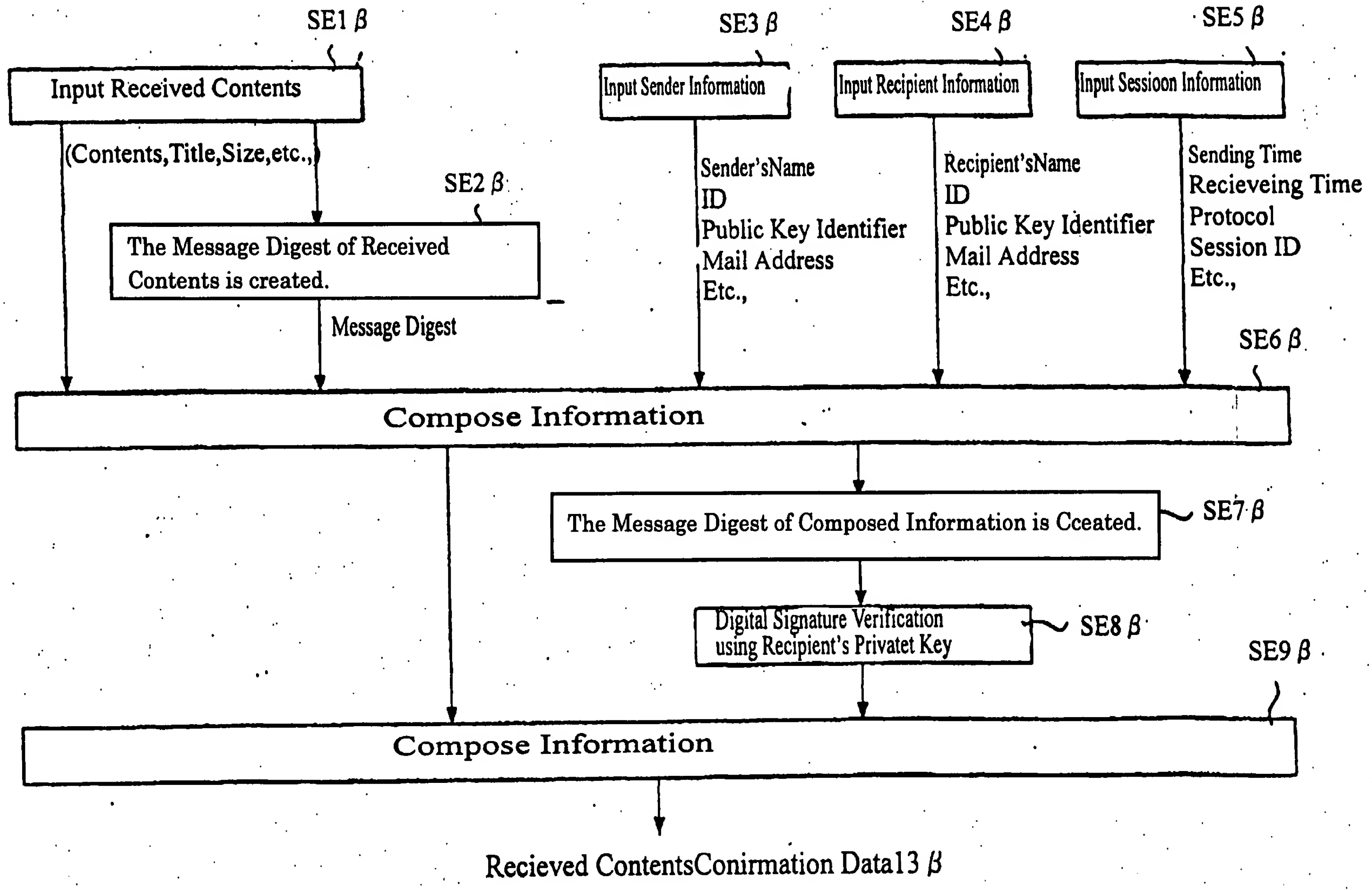

SE1 β
SE3 β
SE4 β
SE5 β
Input Received Contents
Input Sender Information
Input Recipient Information
Input Sessioon Information
(Contents,Title,Size,etc.,)
SE2 β
The Message Digest of Received Contents is created.
Message Digest
Sender'sName
ID
Public Key Identifier
Mail Address
Etc.,
Recipient'sName
ID
Public Key Identifier
Mail Address
Etc.,
Sending Time
Recieveing Time
Protocol
Session ID
Etc.,
SE6 β
Compose Information
The Message Digest of Composed Information is Cceated.
SE7 β
Digital Signature Verification using Recipient's Privatet Key
SE8 β
SE9 β
Compose Information
Recieved ContentsConirmation Data13 β

FIG16

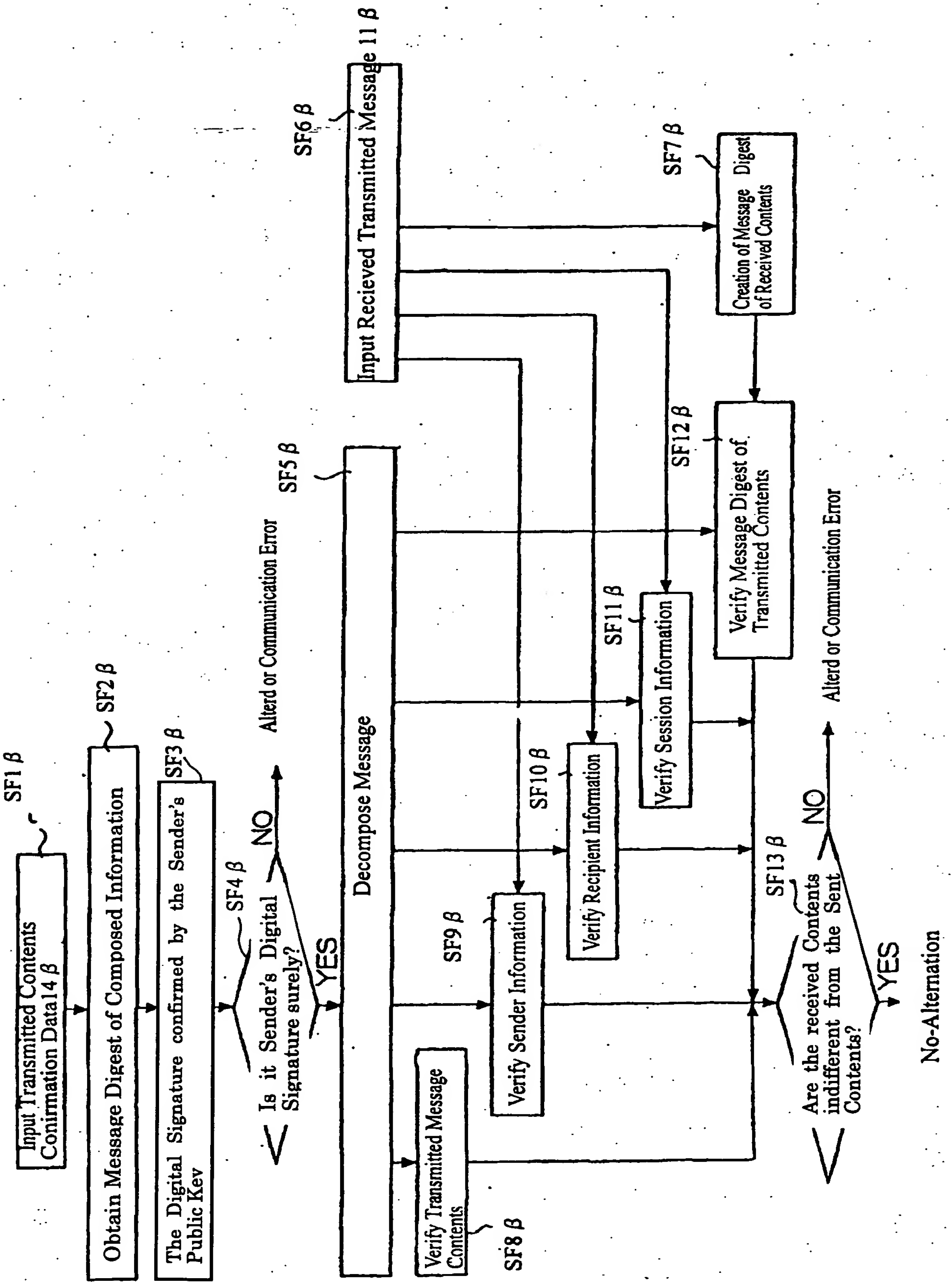

SF1 β
Input Transmitted Contents Conirmation Data14 β
SF2 β
Obtain Message Digest of Composed Information
SF3 β
The Digital Signature confirmed by the Sender's Public Kev
SF4 β
Is it Sender's Digital Signature surely?
NO
Alterd or Communication Error
YES
SF5 β
Decompose Message
SF6 β
Input Recieved Transmitted Message 11 β
SF7 β
Creation of Message Digest of Received Contents
SF8 β
Verify Transmitted Message Contents
SF9 β
Verify Sender Information
SF10 β
Verify Recipient Information
SF11 β
Verify Session Information
SF12 β
Verify Message Digest of Transmitted Contents
SF13 β
Are the received Contents indifferent from the Sent Contents?
NO
Alterd or Communication Error
YES
No-Alternation

FIG17

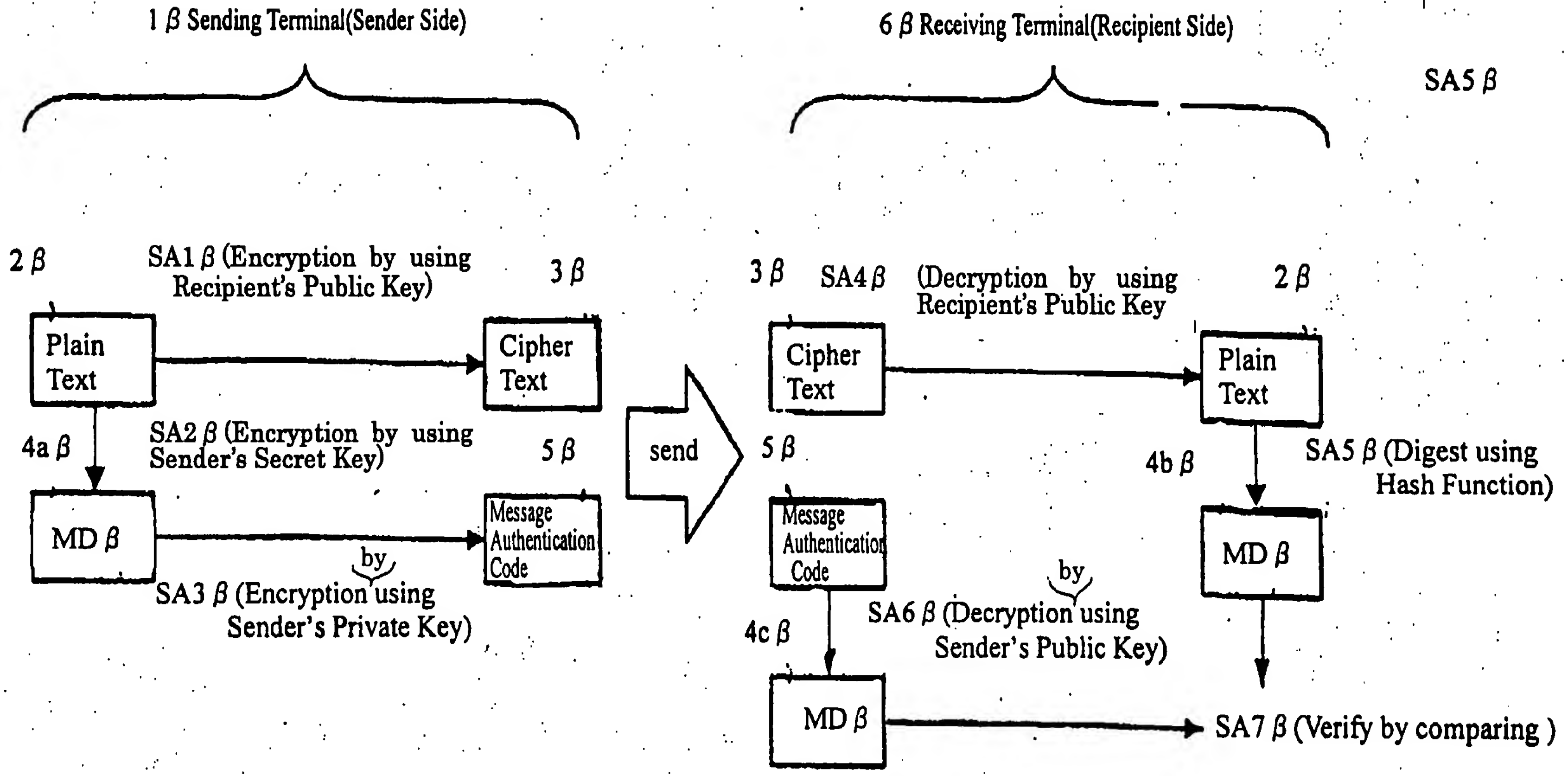

1 β Sending Terminal(Sender Side)
6 β Receiving Terminal(Recipient Side)
SA5 β
2 β
SA1 β (Encryption by using Recipient's Public Key)
3 β
Plain Text
Cipher Text
4a β
SA2 β (Encryption by using Sender's Secret Key)
5 β
MD β
by
SA3 β (Encryption using Sender's Private Key)
Message Authentication Code
send
3 β
SA4 β
(Decryption by using Recipient's Public Key
2 β
Cipher Text
Plain Text
5 β
4b β
SA5 β (Digest using Hash Function)
Message Authentication Code
MD β
by
SA6 β (Decryption using Sender's Public Key)
4c β
MD β
SA7 β (Verify by comparing)

FIG18

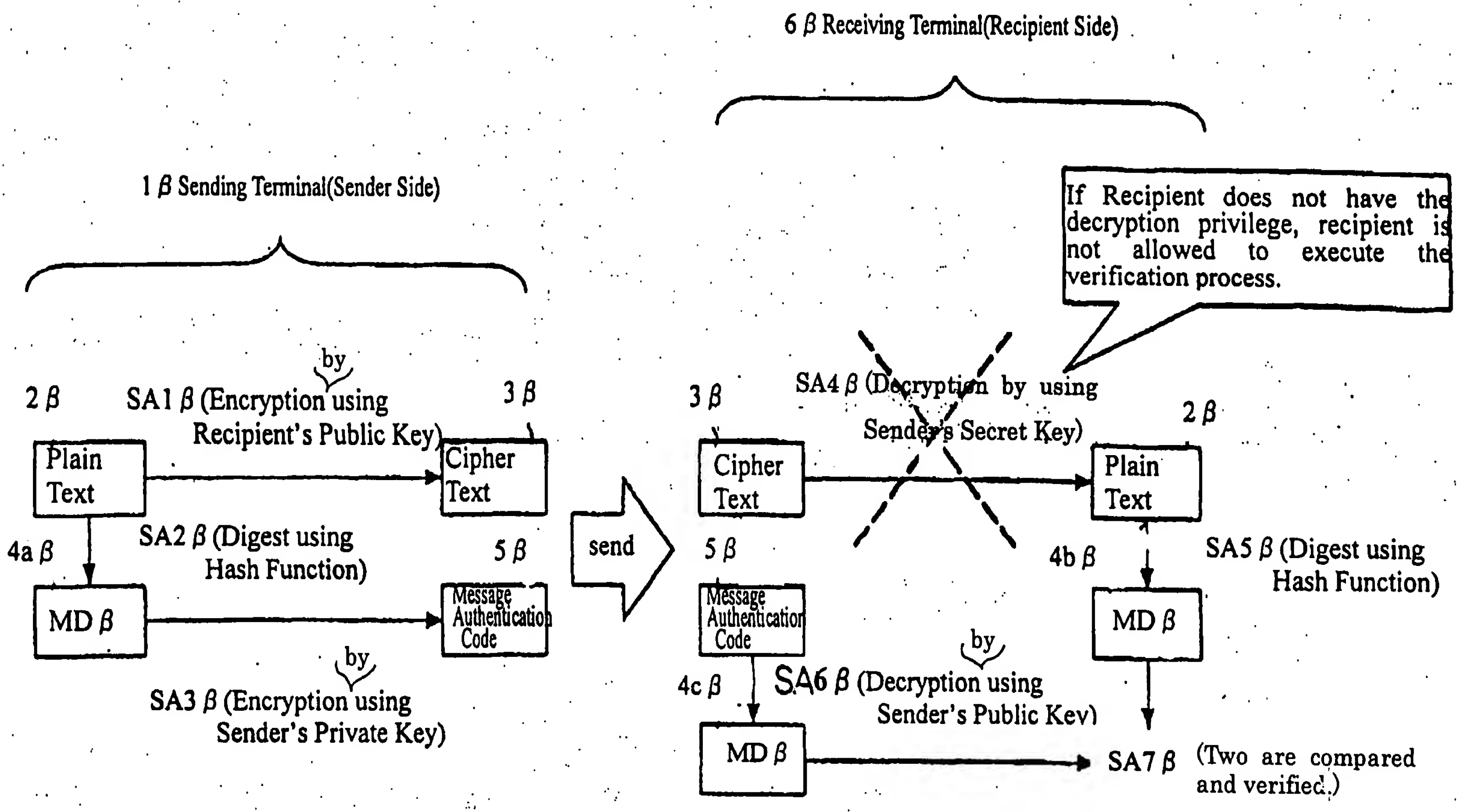

6 β Receiving Terminal(Recipient Side)
1 β Sending Terminal(Sender Side)
If Recipient does not have the decryption privilege, recipient is not allowed to execute the verification process.
2 β
SA1 β (Encryption using Recipient's Public Key)
by
3 β
Plain Text
Cipher Text
4a β
SA2 β (Digest using Hash Function)
5 β
MD β
Message Authentication Code
SA3 β (Encryption using Sender's Private Key)
by
send
3 β
Cipher Text
SA4 β (Decryption by using Sender's Secret Key)
2 β
Plain Text
5 β
Message Authentication Code
4b β
SA5 β (Digest using Hash Function)
MD β
4c β
SA6 β (Decryption using Sender's Public Kev)
by
MD β
SA7 β
(Two are compared and verified.)

FIG.19

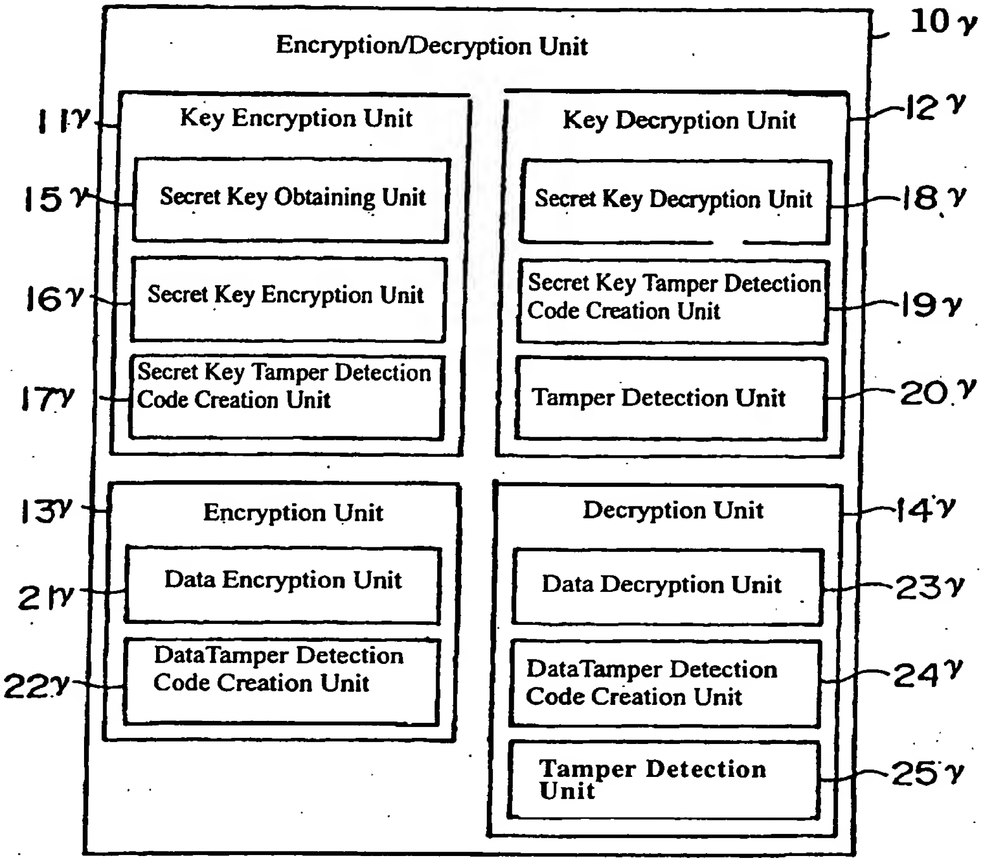

Encryption/Decryption Unit
10
Key Encryption Unit
11
Secret Key Obtaining Unit
15
Secret Key Encryption Unit
16
Secret Key Tamper Detection Code Creation Unit
17
Key Decryption Unit
12
Secret Key Decryption Unit
18
Secret Key Tamper Detection Code Creation Unit
19
Tamper Detection Unit
20
Encryption Unit
13
Data Encryption Unit
21
DataTamper Detection Code Creation Unit
22
Decryption Unit
14
Data Decryption Unit
23
DataTamper Detection Code Creation Unit
24
Tamper Detection Unit
25

FIG20

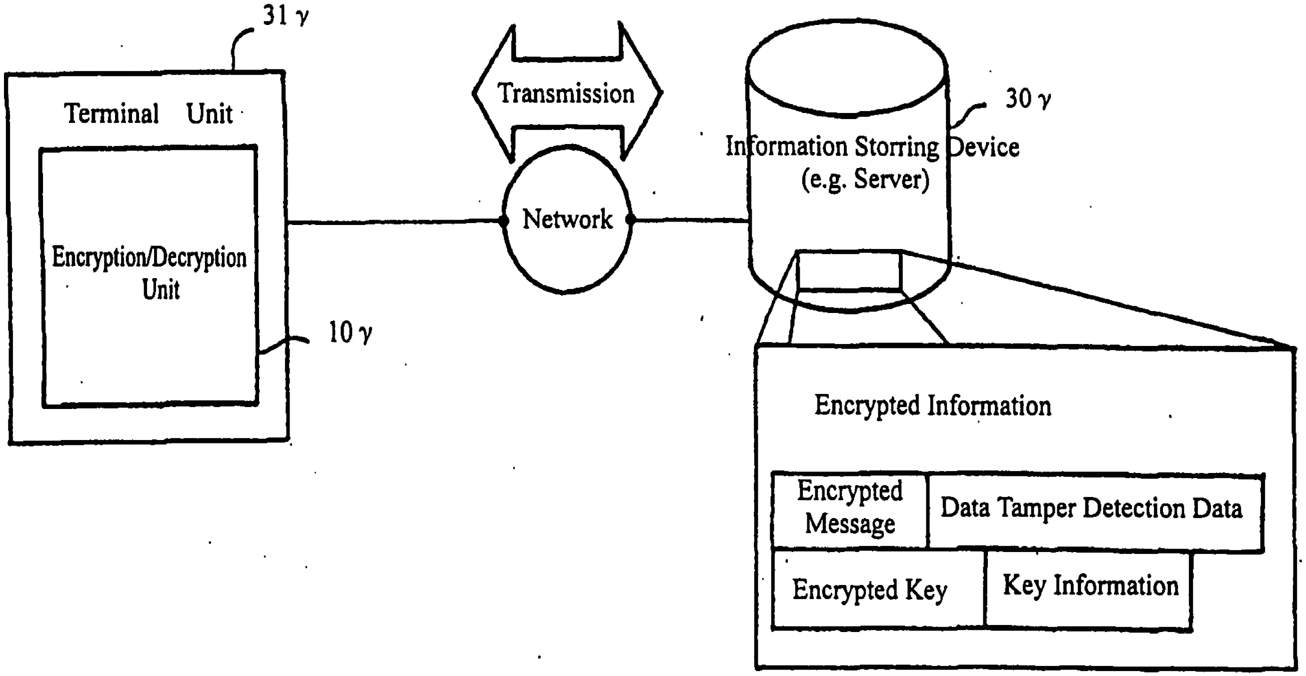
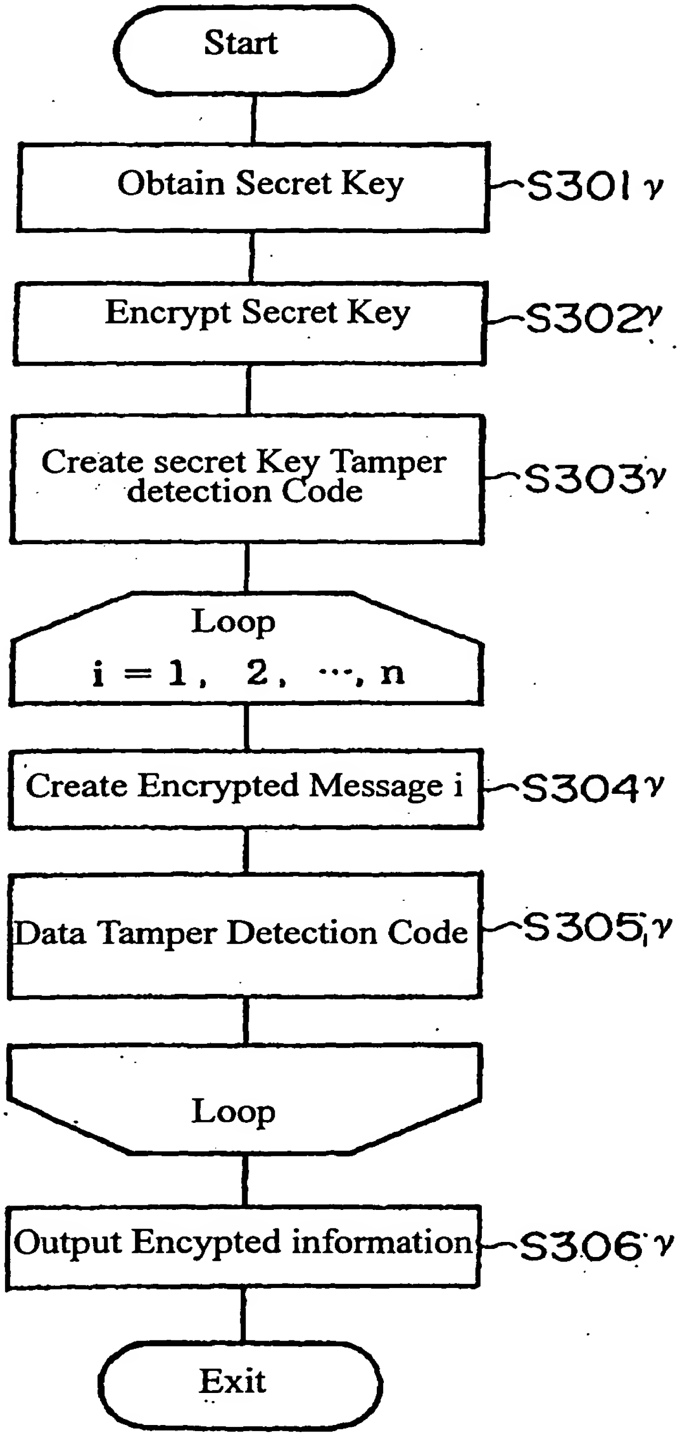

31γ
Terminal Unit
Encryption/Decryption Unit
10γ
Transmission
Network
30γ
Information Storring Device (e.g. Server)
Encrypted Information
Encrypted Message
Data Tamper Detection Data
Encrypted Key
Key Information

FIG.21


Start
Obtain Secret Key
S301
Encrypt Secret Key
S302
Create secret Key Tamper detection Code
S303
Loop
i = 1, 2, ···, n
Create Encrypted Message i
S304
Data Tamper Detection Code
S305
Loop
Output Encypted information
S306
Exit

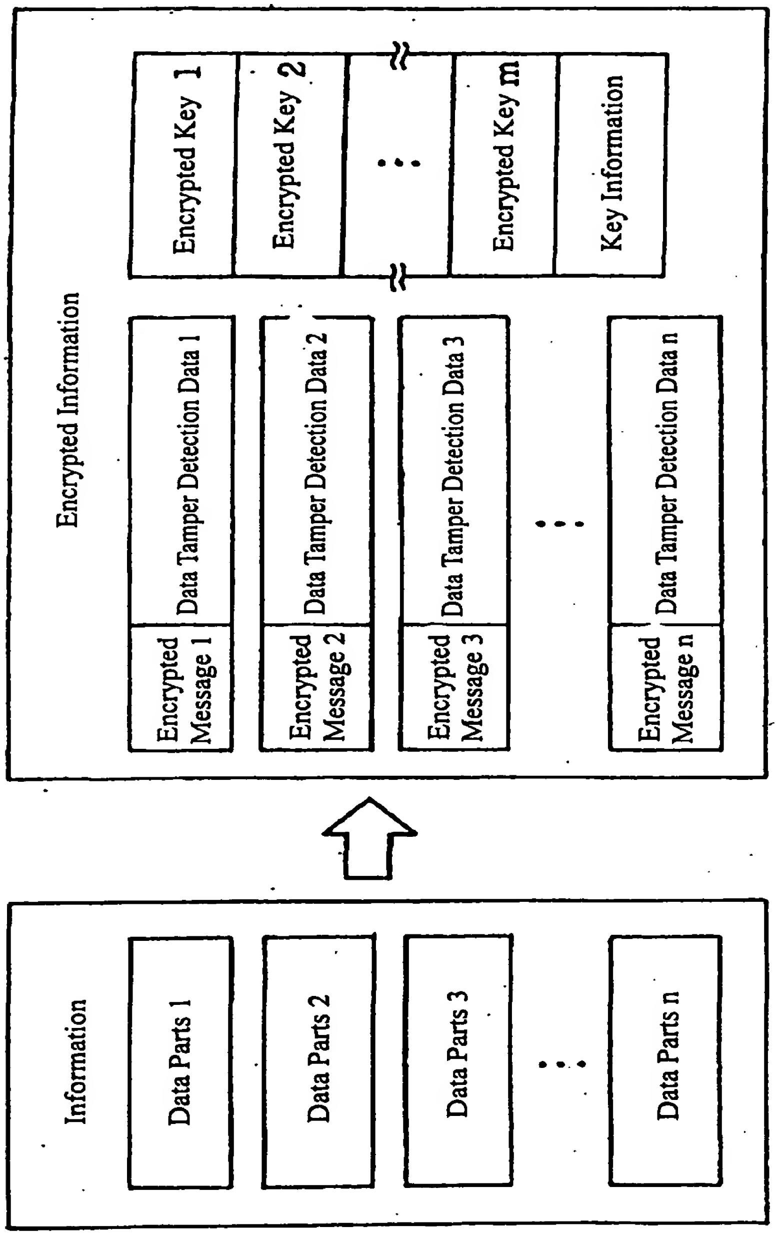

Information
Data Parts 1
Data Parts 2
Data Parts 3
...
Data Parts n
Encrypted Information
Encrypted Message 1
Data Tamper Detection Data 1
Encrypted Message 2
Data Tamper Detection Data 2
Encrypted Message 3
Data Tamper Detection Data 3
...
Encrypted Message n
Data Tamper Detection Data n
Encrypted Key 1
Encrypted Key 2
...
Encrypted Key m
Key Information

FIG22

FIG.23

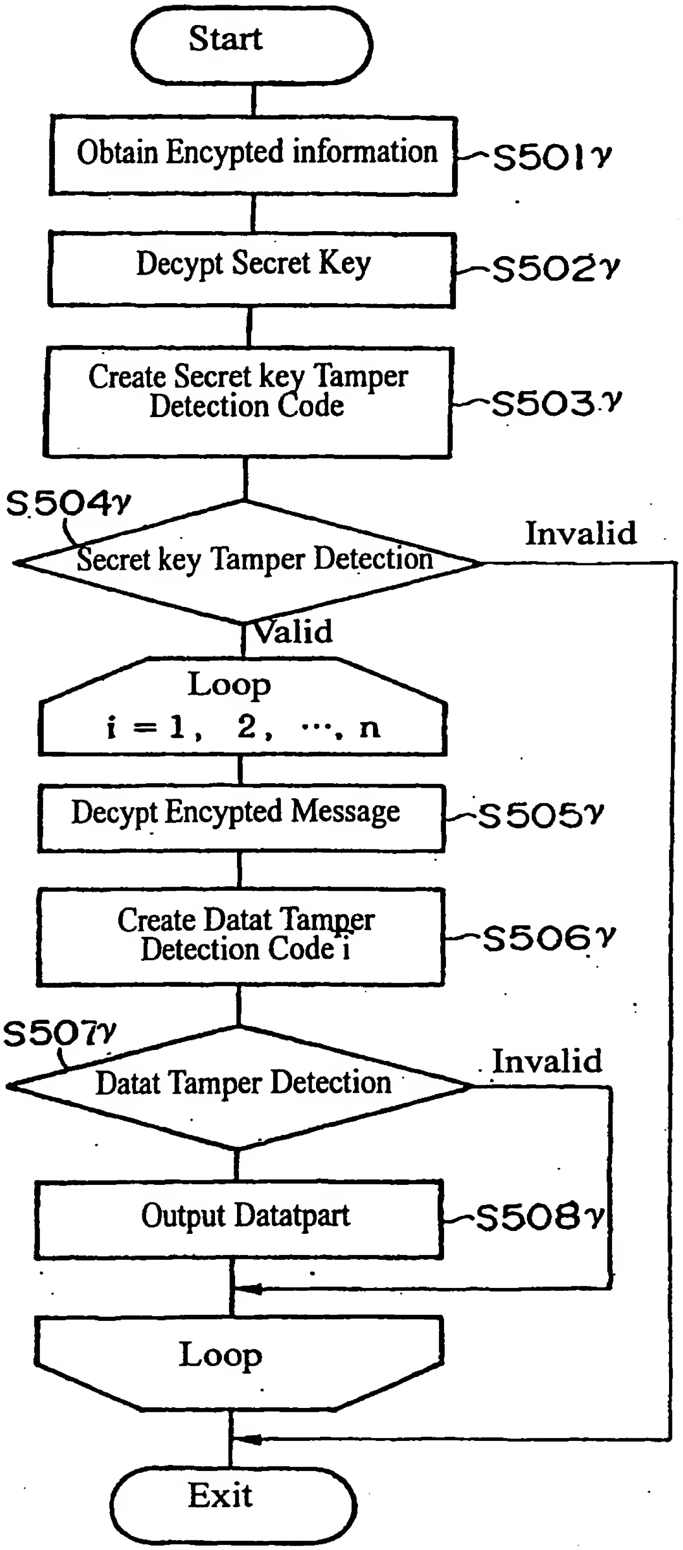

Start
Obtain Encypted information
S501
Decypt Secret Key
S502
Create Secret key Tamper Detection Code
S503
S504
Secret key Tamper Detection
Invalid
Valid
Loop
i = 1, 2, ···, n
Decypt Encypted Message
S505
Create Datat Tamper Detection Code i
S506
S507
Datat Tamper Detection
Invalid
Output Datatpart
S508
Loop
Exit

FIG.24

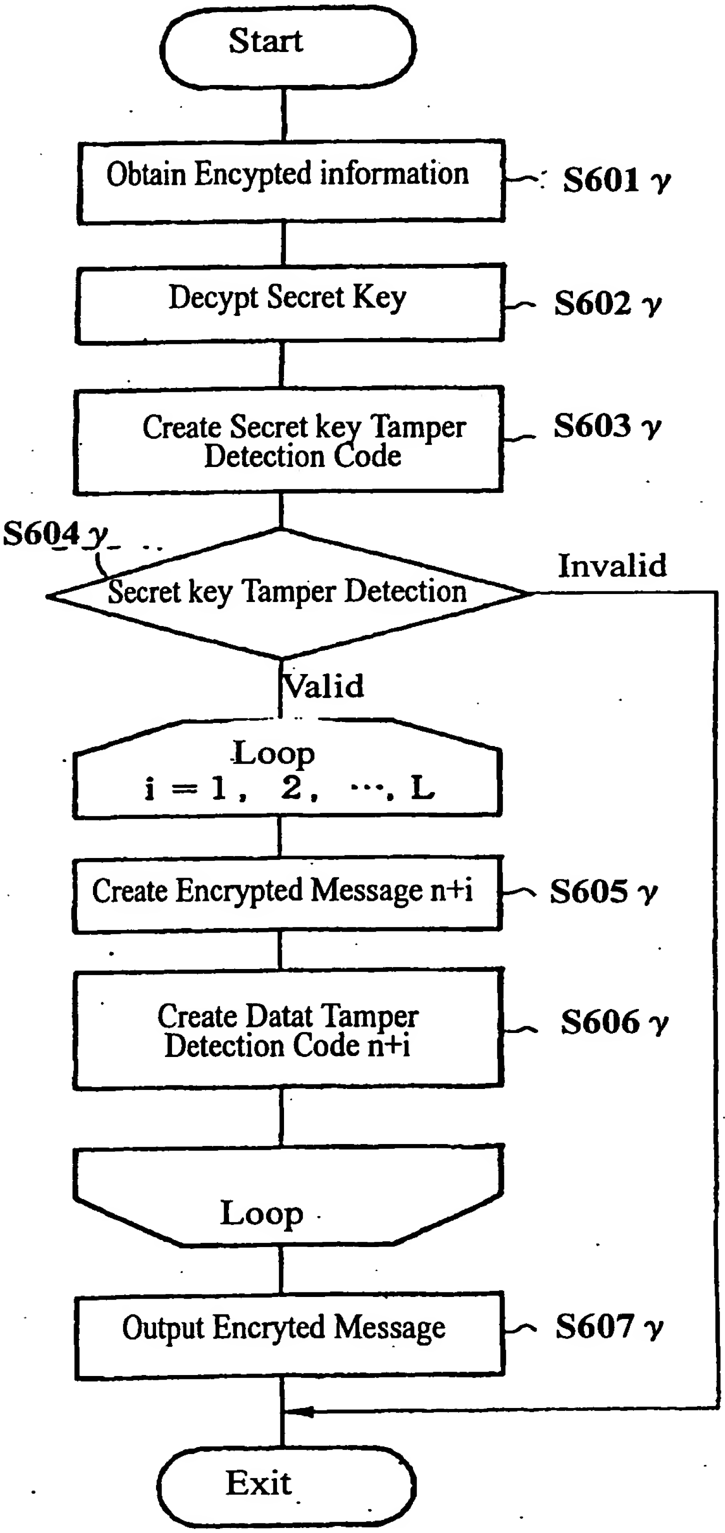

Start
Obtain Encypted information
S601
Decypt Secret Key
S602
Create Secret key Tamper Detection Code
S603
S604
Secret key Tamper Detection
Invalid
Valid
Loop
i = 1, 2, ···, L
Create Encrypted Message n+i
S605
Create Datat Tamper Detection Code n+i
S606
Loop
Output Encryted Message
S607
Exit

FIG25

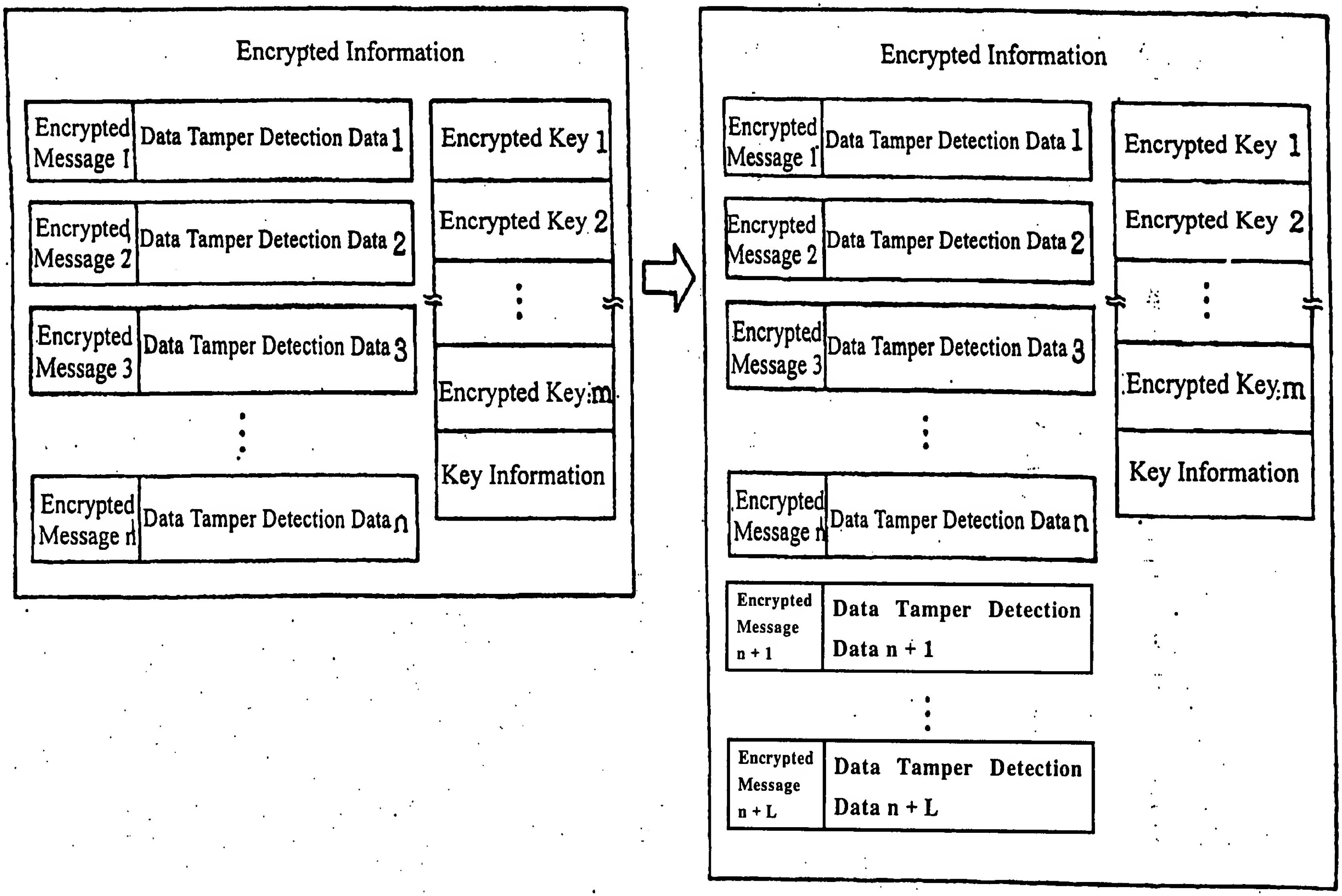
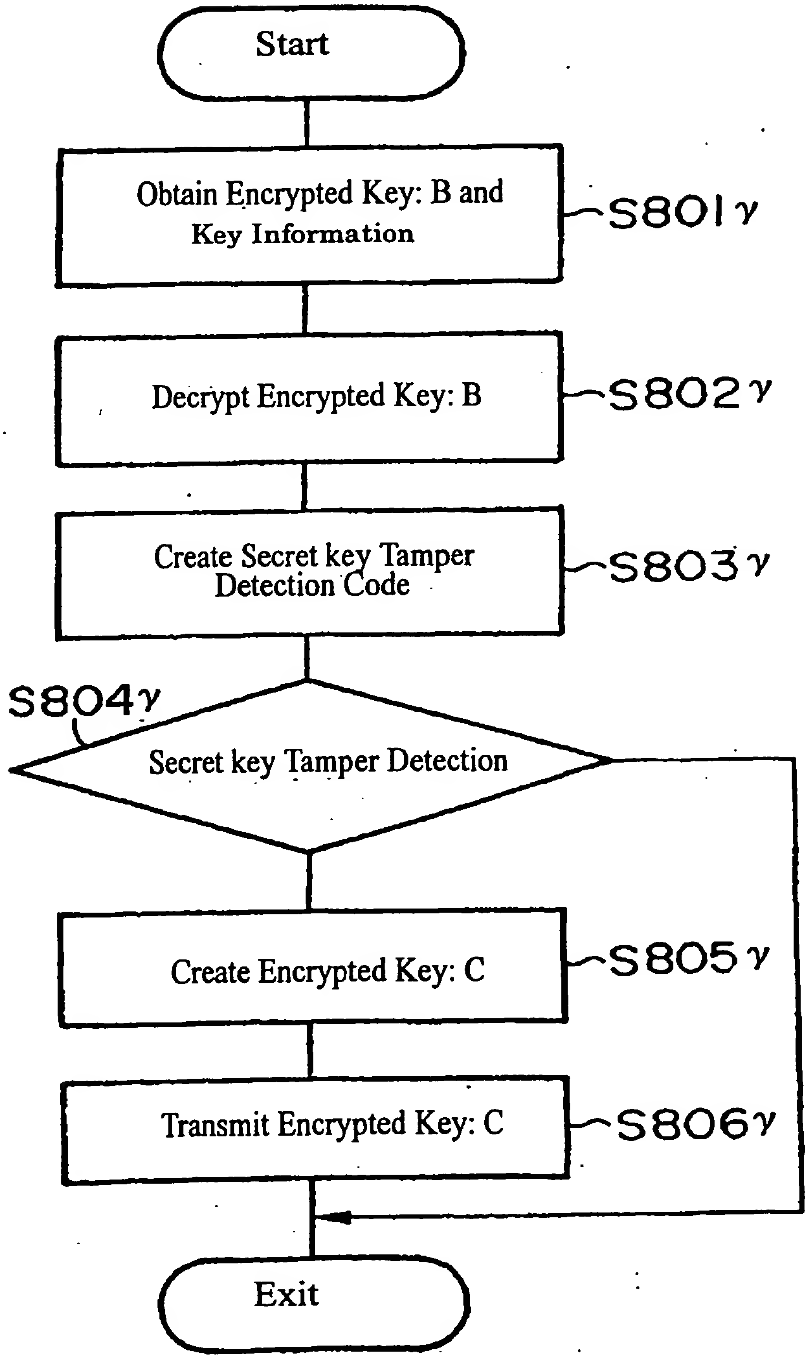

Encrypted Information
Encrypted Message 1
Data Tamper Detection Data 1
Encrypted Message 2
Data Tamper Detection Data 2
Encrypted Message 3
Data Tamper Detection Data 3
Encrypted Message n
Data Tamper Detection Data n
Encrypted Key 1
Encrypted Key 2
Encrypted Key m
Key Information
Encrypted Information
Encrypted Message 1
Data Tamper Detection Data 1
Encrypted Message 2
Data Tamper Detection Data 2
Encrypted Message 3
Data Tamper Detection Data 3
Encrypted Message n
Data Tamper Detection Data n
Encrypted Message n + 1
Data Tamper Detection Data n + 1
Encrypted Message n + L
Data Tamper Detection Data n + L
Encrypted Key 1
Encrypted Key 2
Encrypted Key m
Key Information

FIG.26


Start
Obtain Encrypted Key: B and Key Information
S801
Decrypt Encrypted Key: B
S802
Create Secret key Tamper Detection Code
S803
S804
Secret key Tamper Detection
Create Encrypted Key: C
S805
Transmit Encrypted Key: C
S806
Exit

09/700390

OBLON ET AL (703) 413-3000
DOCKET # 196191US2PCT SHEET 27 OF 73

FIG27

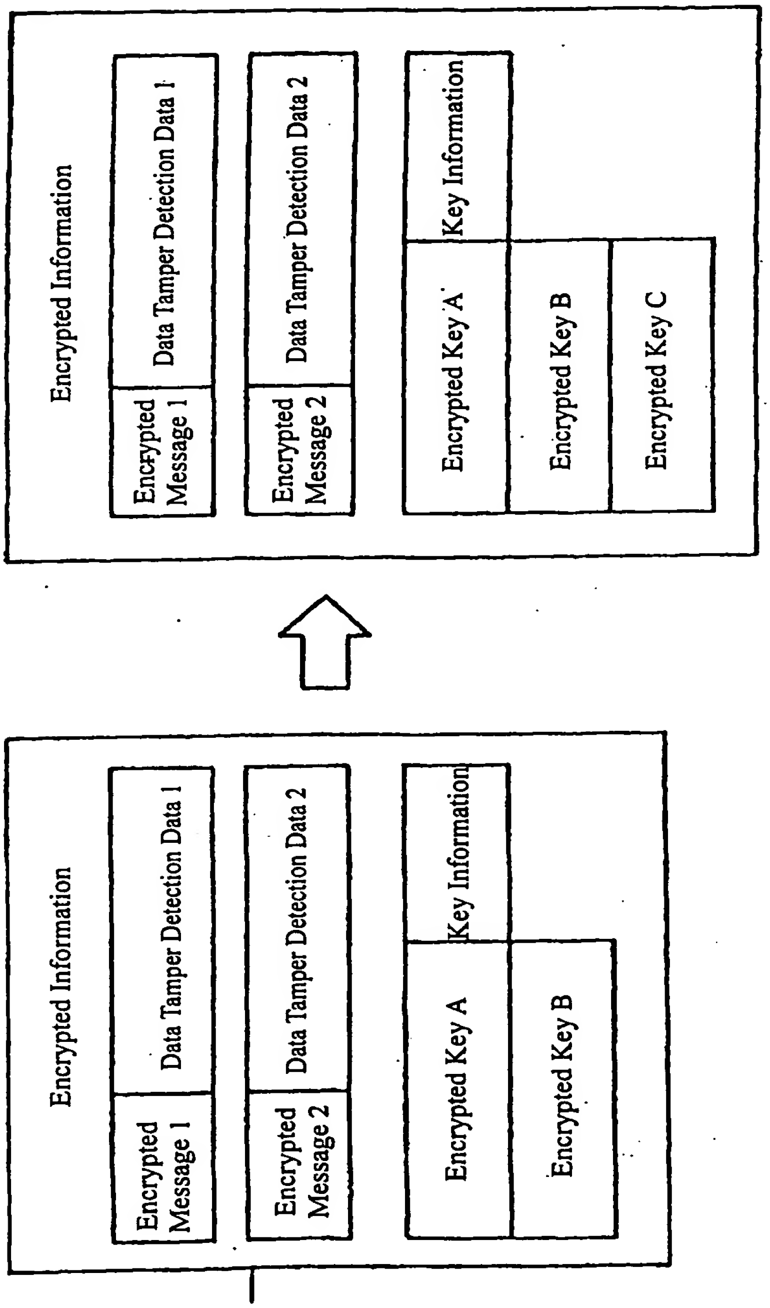


FIG.28

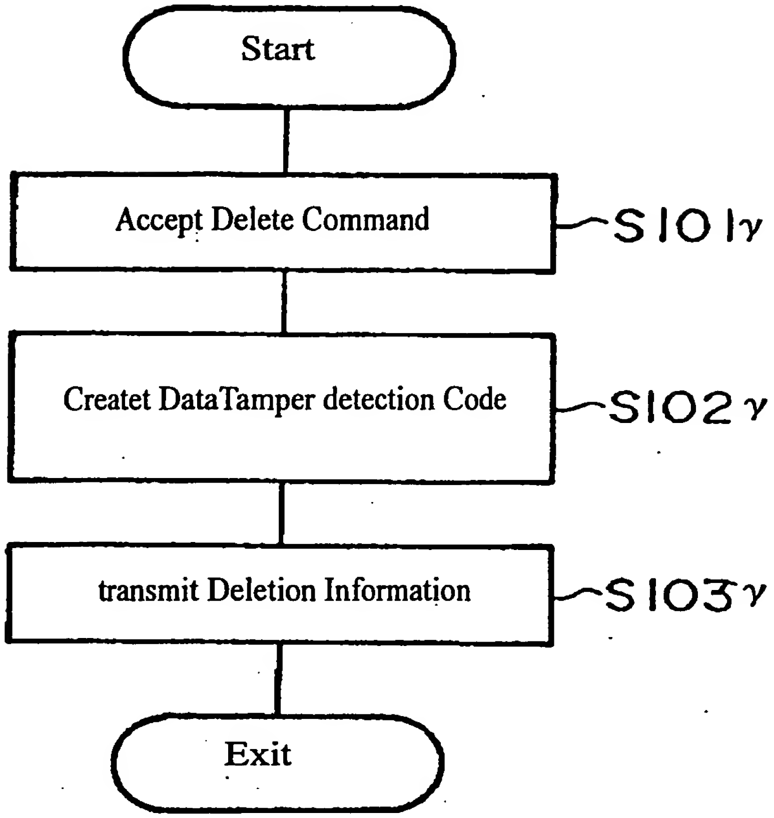

Start
Accept Delete Command
S101
Createt DataTamper detection Code
S102
transmit Deletion Information
S103
Exit

FIG29

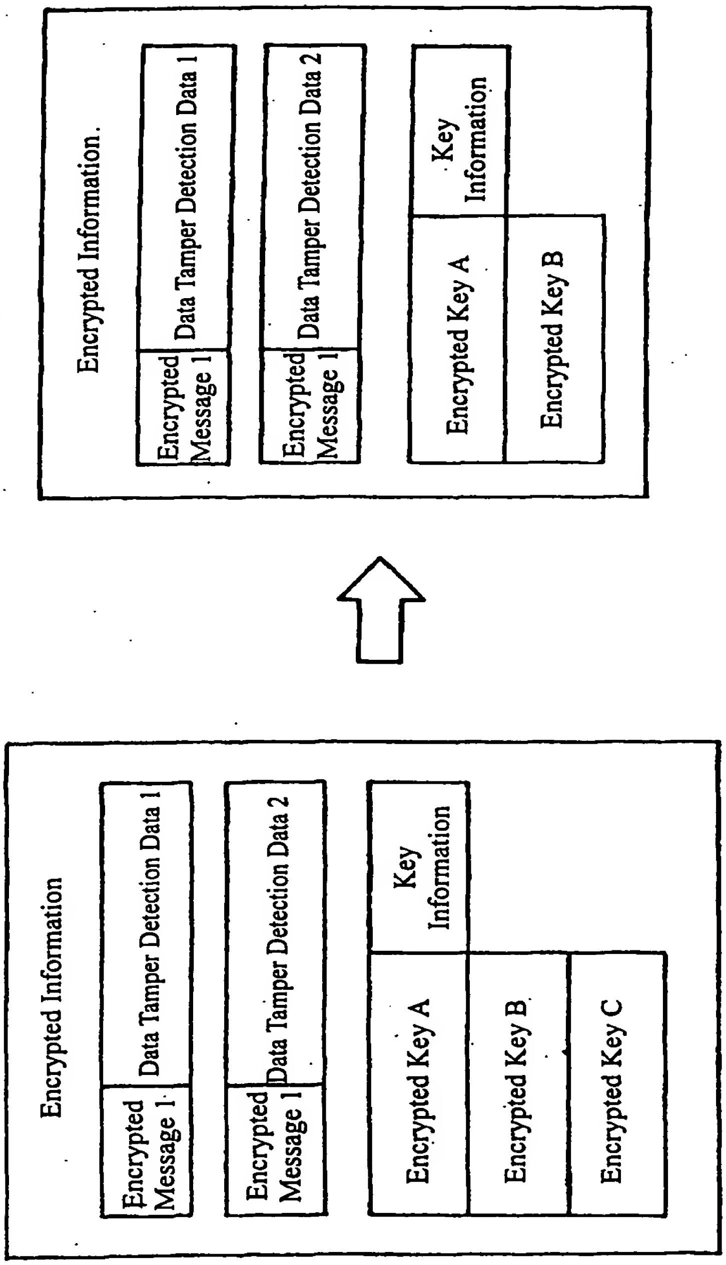

Encrypted Information
Encrypted Message 1
Data Tamper Detection Data 1
Encrypted Message 1
Data Tamper Detection Data 2
Key Information
Encrypted Key A
Encrypted Key B
Encrypted Key C
Encrypted Information.
Encrypted Message 1
Data Tamper Detection Data 1
Encrypted Message 1
Data Tamper Detection Data 2
Key Information
Encrypted Key A
Encrypted Key B

FIG.30

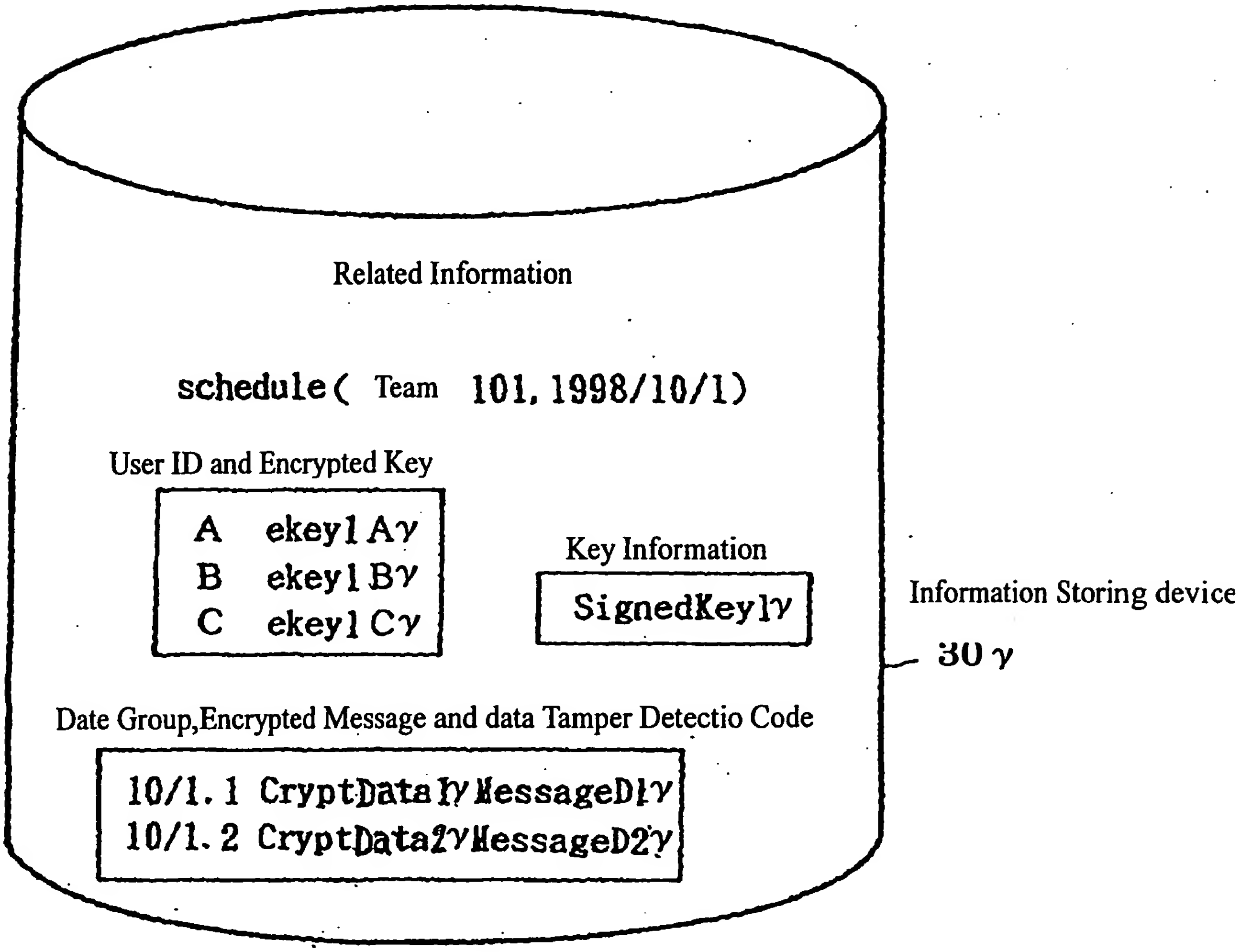
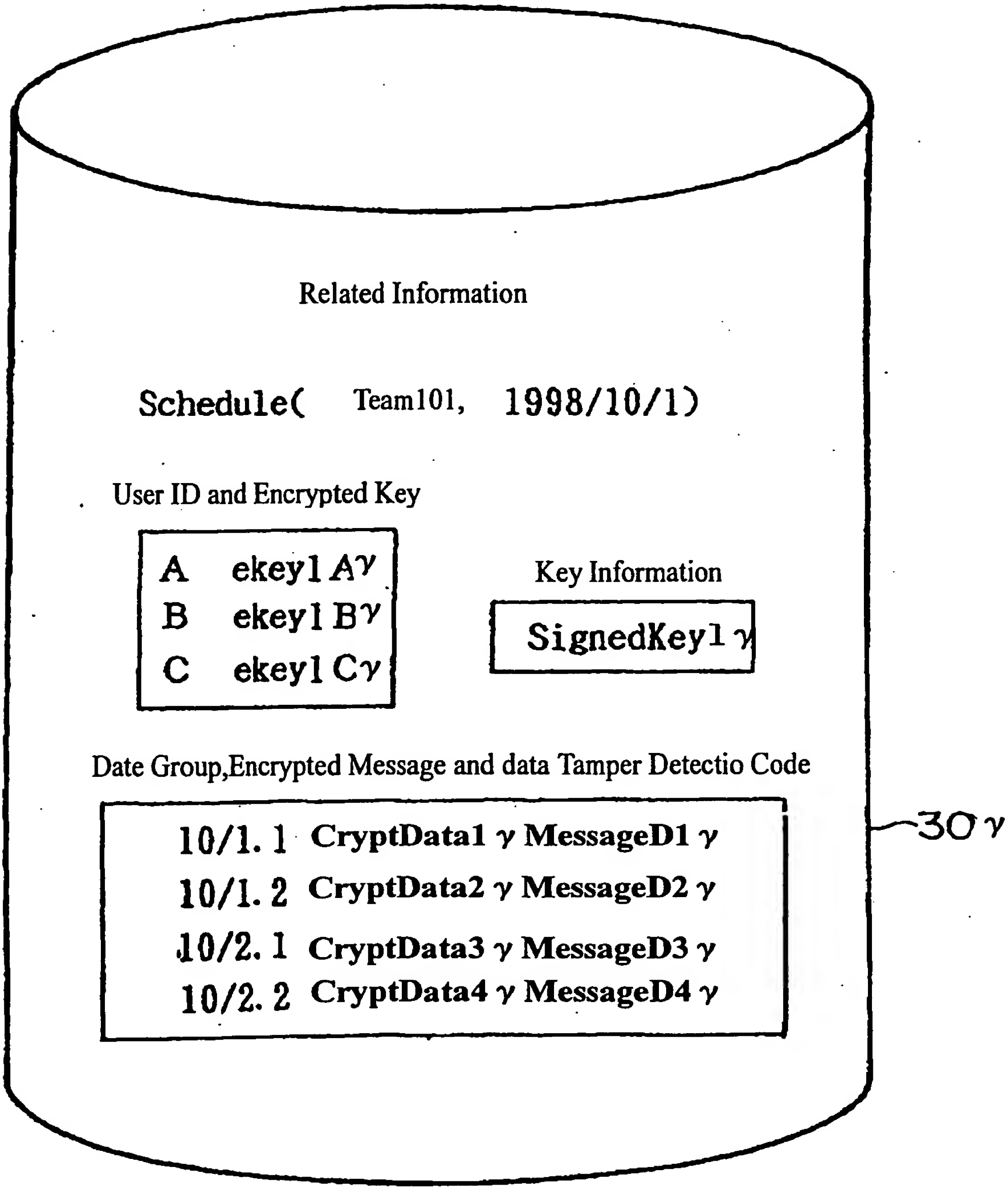

Related Information
schedule(Team 101, 1998/10/1)
User ID and Encrypted Key
A ekey1 Aγ
B ekey1 Bγ
C ekey1 Cγ
Key Information
SignedKey1γ
Information Storing device
30γ
Date Group,Encrypted Message and data Tamper Detectio Code
10/1.1 CryptData1γ MessageD1γ
10/1.2 CryptData2γ MessageD2γ

FIG.31



Related Information

Schedule(Team101, 1998/10/1)

User ID and Encrypted Key

A	ekey1 Aγ
B	ekey1 Bγ
C	ekey1 Cγ

Key Information

SignedKey1 γ

Date Group,Encrypted Message and data Tamper Detectio Code

10/1. 1	CryptData1 γ	MessageD1 γ
10/1. 2	CryptData2 γ	MessageD2 γ
10/2. 1	CryptData3 γ	MessageD3 γ
10/2. 2	CryptData4 γ	MessageD4 γ

FIG.32

Team101 : Schedule

Oct.

1 B: Go to Seminar 15:00~	2 A:Meeting 17:00~	

FIG.33

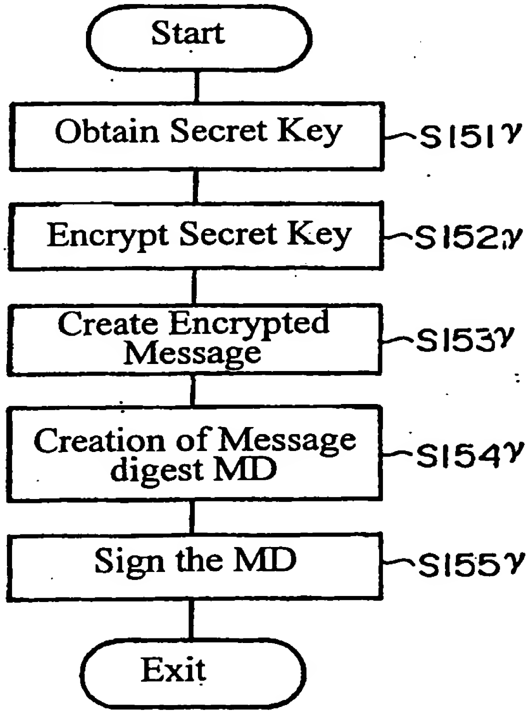


FIG.34

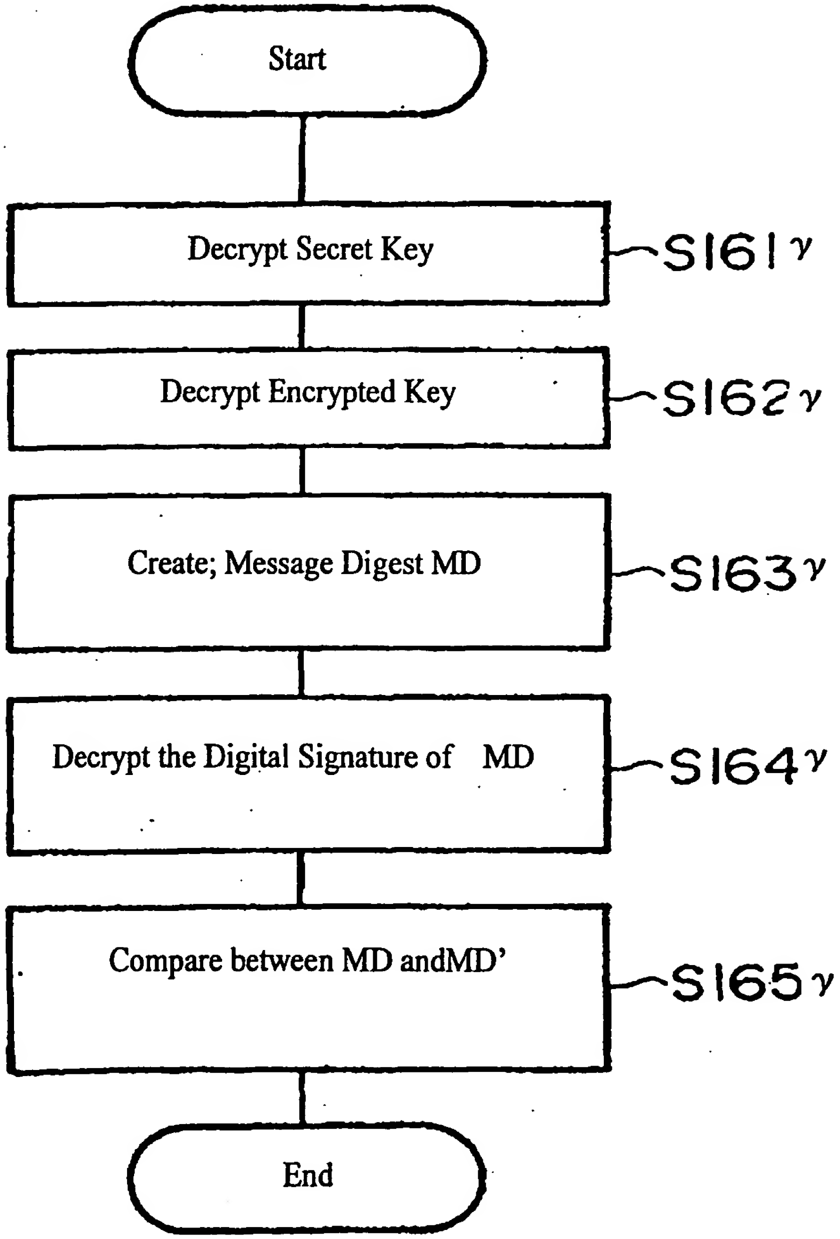

Start
Decrypt Secret Key
S161
Decrypt Encrypted Key
S162
Create; Message Digest MD
S163
Decrypt the Digital Signature of MD
S164
Compare between MD andMD'
S165
End

FIG.35

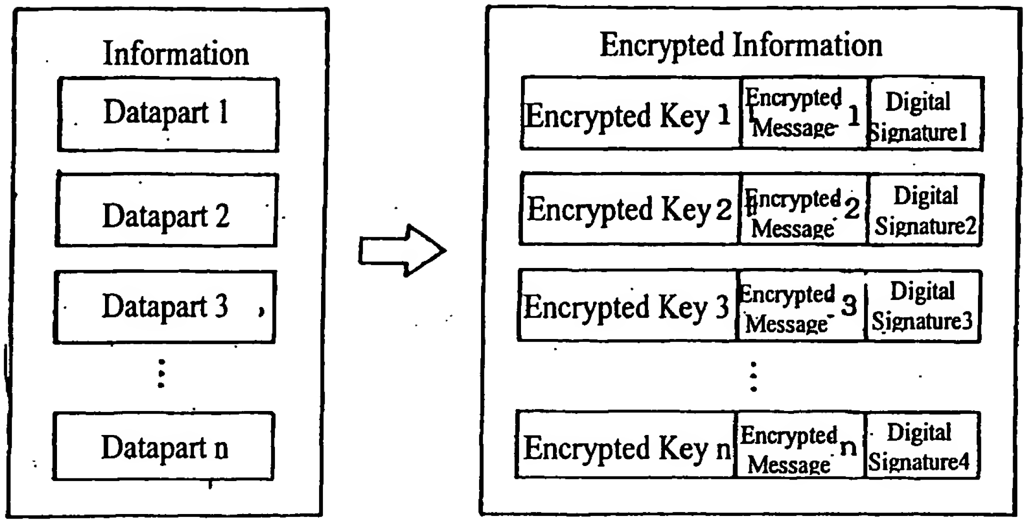

Information
Datapart 1
Datapart 2
Datapart 3
Datapart n
Encrypted Information
Encrypted Key 1
Encrypted Message 1
Digital Signature1
Encrypted Key 2
Encrypted Message 2
Digital Signature2
Encrypted Key 3
Encrypted Message 3
Digital Signature3
Encrypted Key n
Encrypted Message n
Digital Signature4

FIG.36

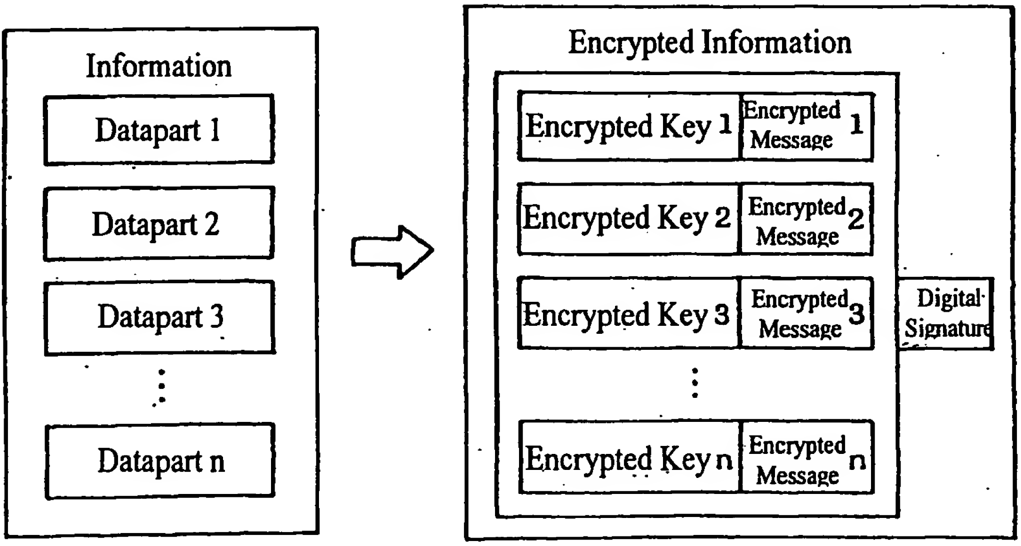

Information
Datapart 1
Datapart 2
Datapart 3
Datapart n
Encrypted Information
Encrypted Key 1
Encrypted Message 1
Encrypted Key 2
Encrypted Message 2
Encrypted Key 3
Encrypted Message 3
Encrypted Key n
Encrypted Message n
Digital Signature

FIG37

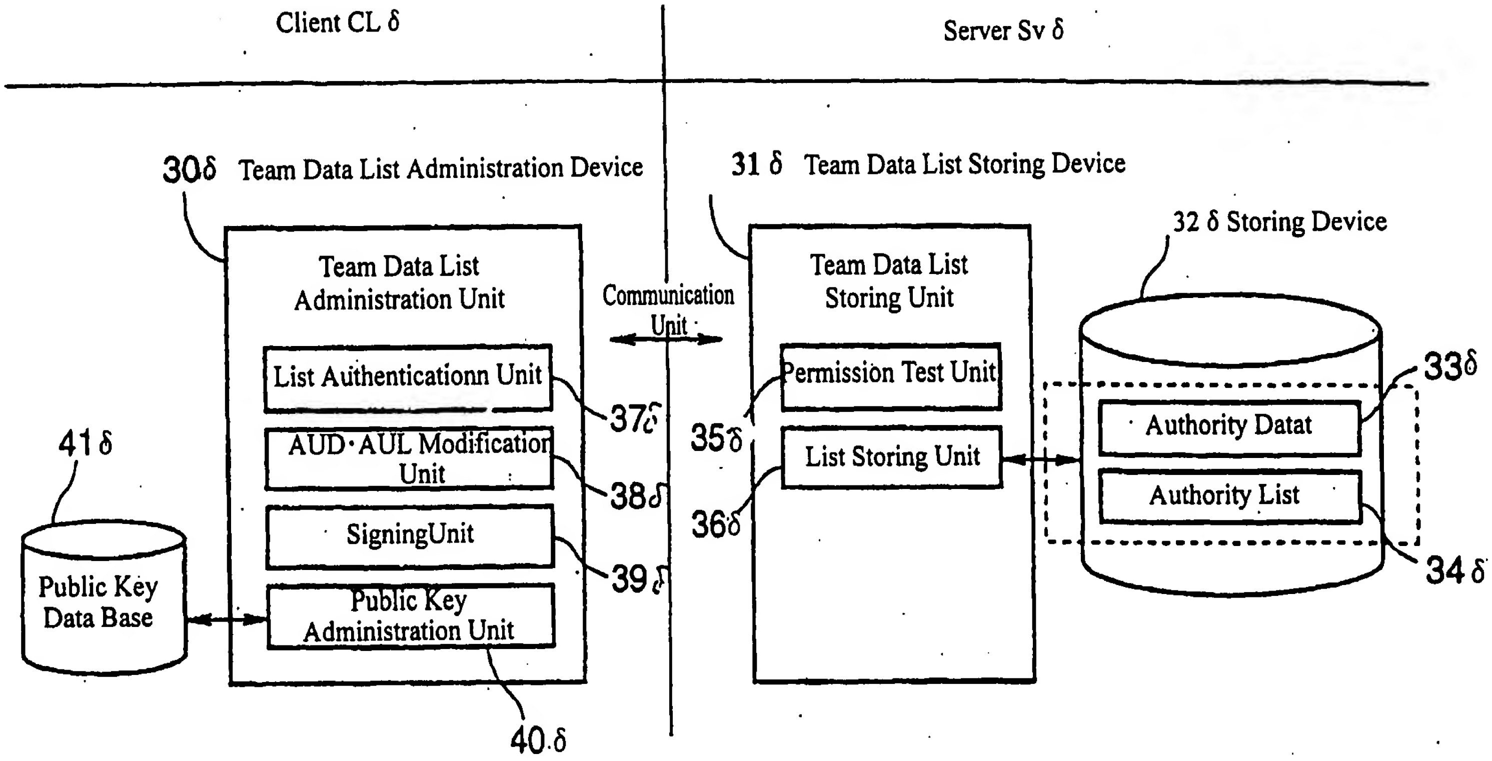
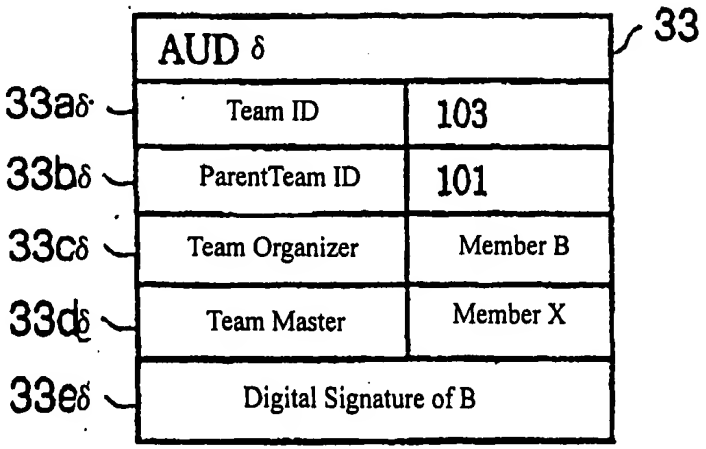
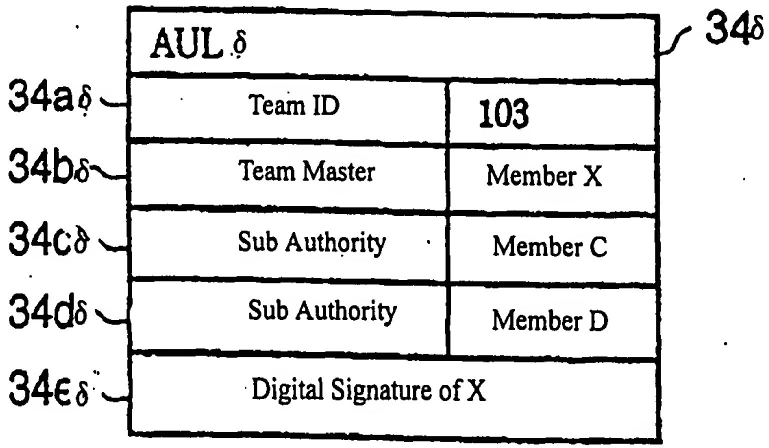

Client CL δ
Server Sv δ
30δ Team Data List Administration Device
31 δ Team Data List Storing Device
32 δ Storing Device
Team Data List Administration Unit
List Authenticationn Unit
AUD·AUL Modification Unit
SigningUnit
Public Key Administration Unit
Communication Unit
Team Data List Storing Unit
Permission Test Unit
List Storing Unit
Authority Datat
Authority List
Public Key Data Base
33δ
34 δ
35δ
36δ
37δ
38δ
39δ
40.δ
41 δ

FIG38A



AUD δ	
Team ID	103
ParentTeam ID	101
Team Organizer	Member B
Team Master	Member X
Digital Signature of B	

FIG38B



AUL δ	
Team ID	103
Team Master	Member X
Sub Authority	Member C
Sub Authority	Member D
Digital Signature of X	

FIG38C

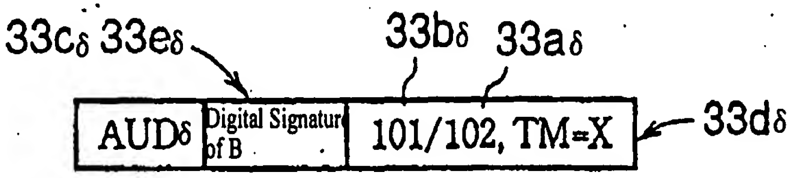


FIG38D

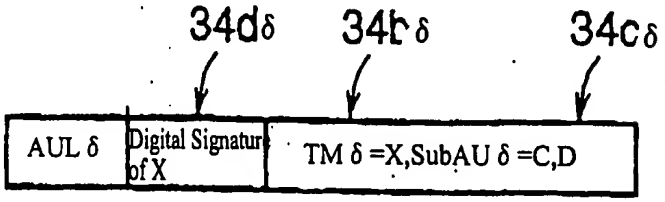


FIG.39

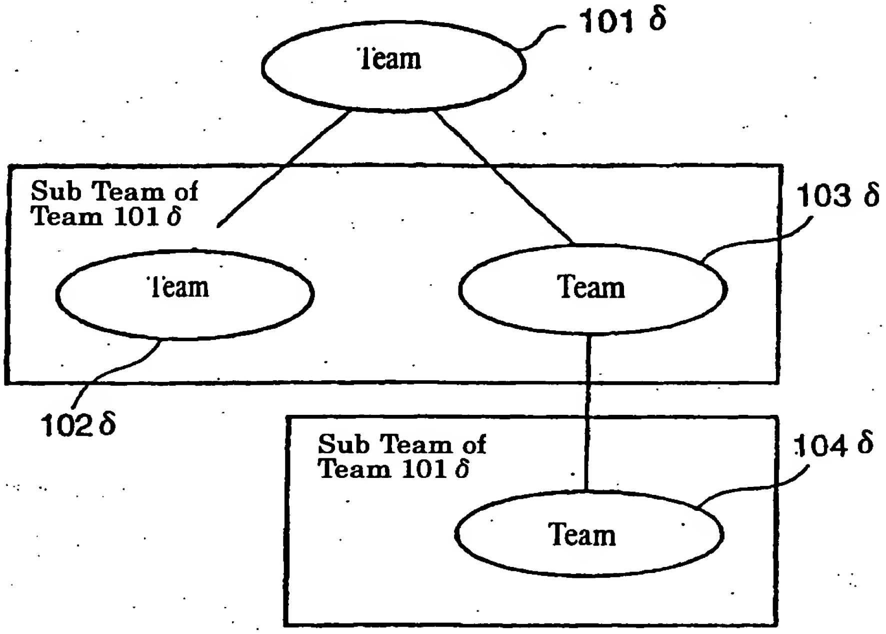
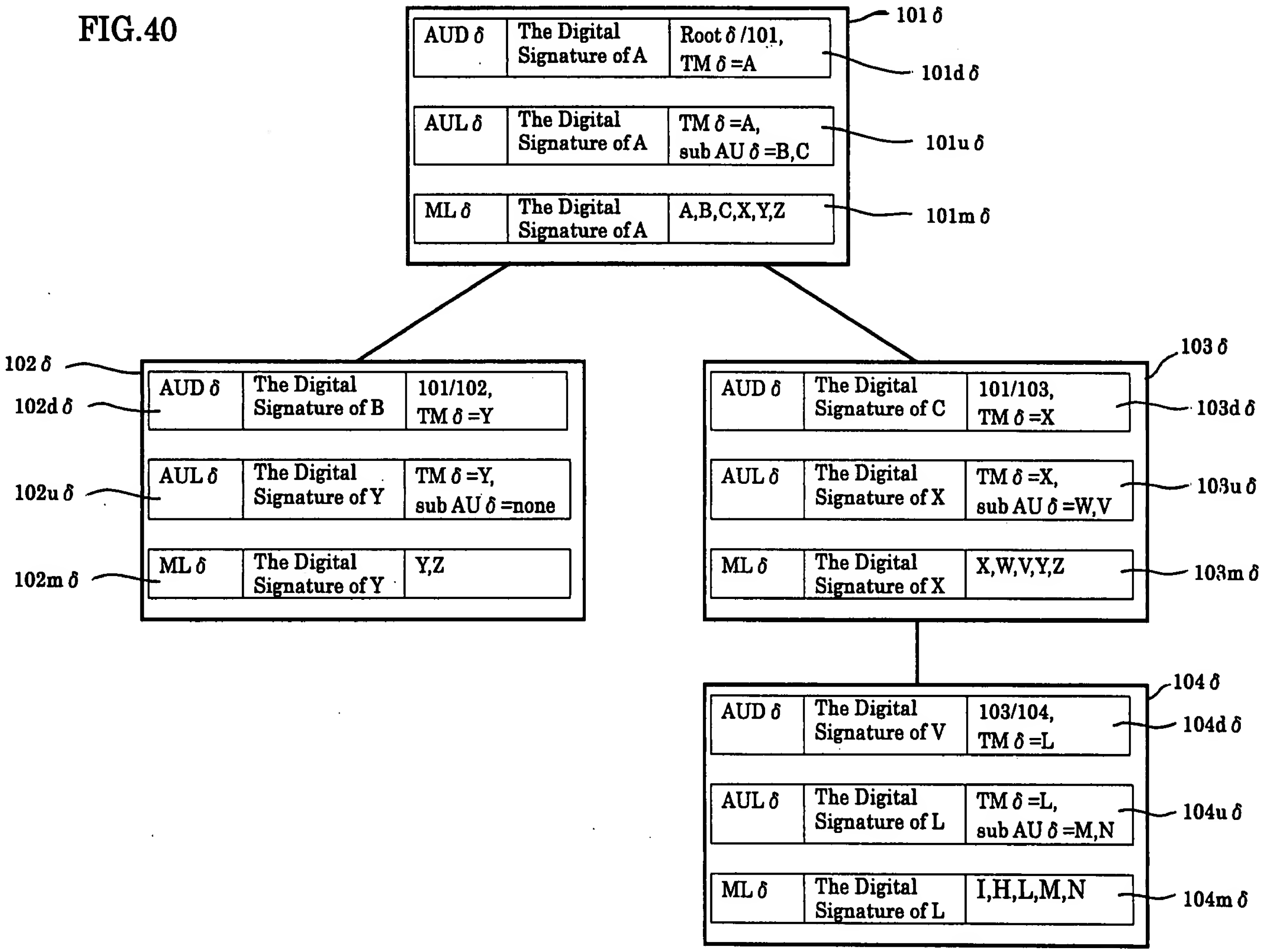

Team
101 δ
Sub Team of Team 101 δ
Team
Team
103 δ
102 δ
Sub Team of Team 101 δ
Team
104 δ

FIG.40


AUD δ
The Digital Signature of A
Root δ /101, TM δ =A
AUL δ
The Digital Signature of A
TM δ =A, sub AU δ =B,C
ML δ
The Digital Signature of A
A,B,C,X,Y,Z
101 δ
101d δ
101u δ
101m δ
AUD δ
The Digital Signature of B
101/102, TM δ =Y
AUL δ
The Digital Signature of Y
TM δ =Y, sub AU δ =none
ML δ
The Digital Signature of Y
Y,Z
102 δ
102d δ
102u δ
102m δ
AUD δ
The Digital Signature of C
101/103, TM δ =X
AUL δ
The Digital Signature of X
TM δ =X, sub AU δ =W,V
ML δ
The Digital Signature of X
X,W,V,Y,Z
103 δ
103d δ
103u δ
103m δ
AUD δ
The Digital Signature of V
103/104, TM δ =L
AUL δ
The Digital Signature of L
TM δ =L, sub AU δ =M,N
ML δ
The Digital Signature of L
I,H,L,M,N
104 δ
104d δ
104u δ
104m δ

OBLON ET AL (703) 413-3000
DOCKET # 199691US2PCT SHEET 39 OF 73

09/700390

FIG.41

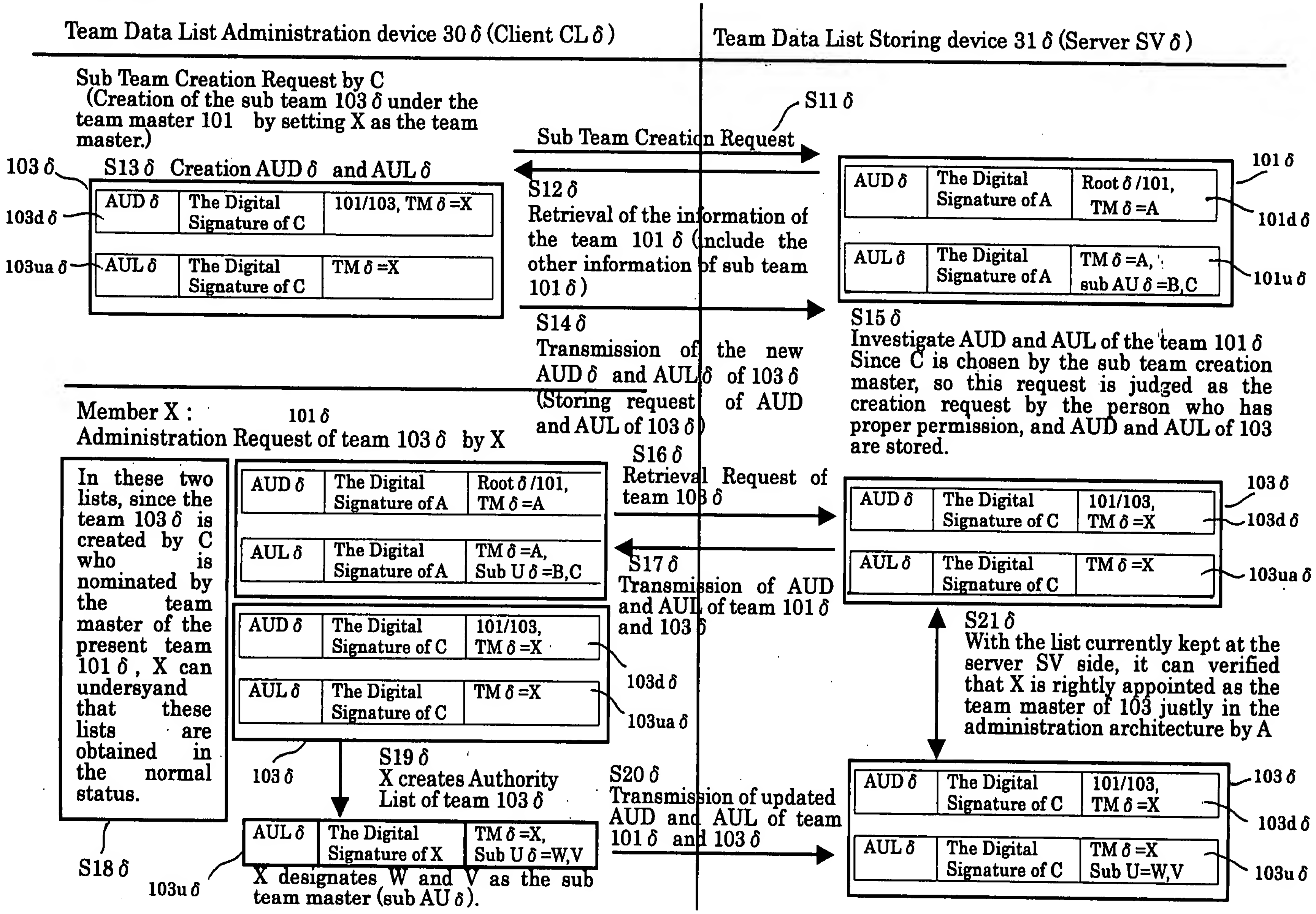

Team Data List Administration device 30 δ (Client CL δ)
Team Data List Storing device 31 δ (Server SV δ)
Sub Team Creation Request by C (Creation of the sub team 103 δ under the team master 101 by setting X as the team master.)
103 δ
S13 δ Creation AUD δ and AUL δ
103d δ
103ua δ
AUD δ | The Digital Signature of C | 101/103, TM δ =X
AUL δ | The Digital Signature of C | TM δ =X
S11 δ
Sub Team Creation Request
S12 δ
Retrieval of the information of the team 101 δ (include the other information of sub team 101 δ)
101 δ
101d δ
101u δ
AUD δ | The Digital Signature of A | Root δ /101, TM δ =A
AUL δ | The Digital Signature of A | TM δ =A, sub AU δ =B,C
S14 δ
Transmission of the new AUD δ and AUL δ of 103 δ (Storing request of AUD and AUL of 103 δ)
S15 δ
Investigate AUD and AUL of the team 101 δ Since C is chosen by the sub team creation master, so this request is judged as the creation request by the person who has proper permission, and AUD and AUL of 103 are stored.
Member X :
101 δ
Administration Request of team 103 δ by X
In these two lists, since the team 103 δ is created by C who is nominated by the team master of the present team 101 δ, X can undersyand that these lists are obtained in the normal status.
S18 δ
AUD δ | The Digital Signature of A | Root δ /101, TM δ =A
AUL δ | The Digital Signature of A | TM δ =A, Sub U δ =B,C
AUD δ | The Digital Signature of C | 101/103, TM δ =X
AUL δ | The Digital Signature of C | TM δ =X
103d δ
103ua δ
103 δ
S16 δ
Retrieval Request of team 103 δ
S17 δ
Transmission of AUD and AUL of team 101 δ and 103 δ
103 δ
103d δ
103ua δ
AUD δ | The Digital Signature of C | 101/103, TM δ =X
AUL δ | The Digital Signature of C | TM δ =X
S19 δ
X creates Authority List of team 103 δ
AUL δ | The Digital Signature of X | TM δ =X, Sub U δ =W,V
103u δ
X designates W and V as the sub team master (sub AU δ).
S20 δ
Transmission of updated AUD and AUL of team 101 δ and 103 δ
S21 δ
With the list currently kept at the server SV side, it can verified that X is rightly appointed as the team master of 103 justly in the administration architecture by A
103 δ
103d δ
103u δ
AUD δ | The Digital Signature of C | 101/103, TM δ =X
AUL δ | The Digital Signature of C | TM δ =X Sub U=W,V

FIG.42

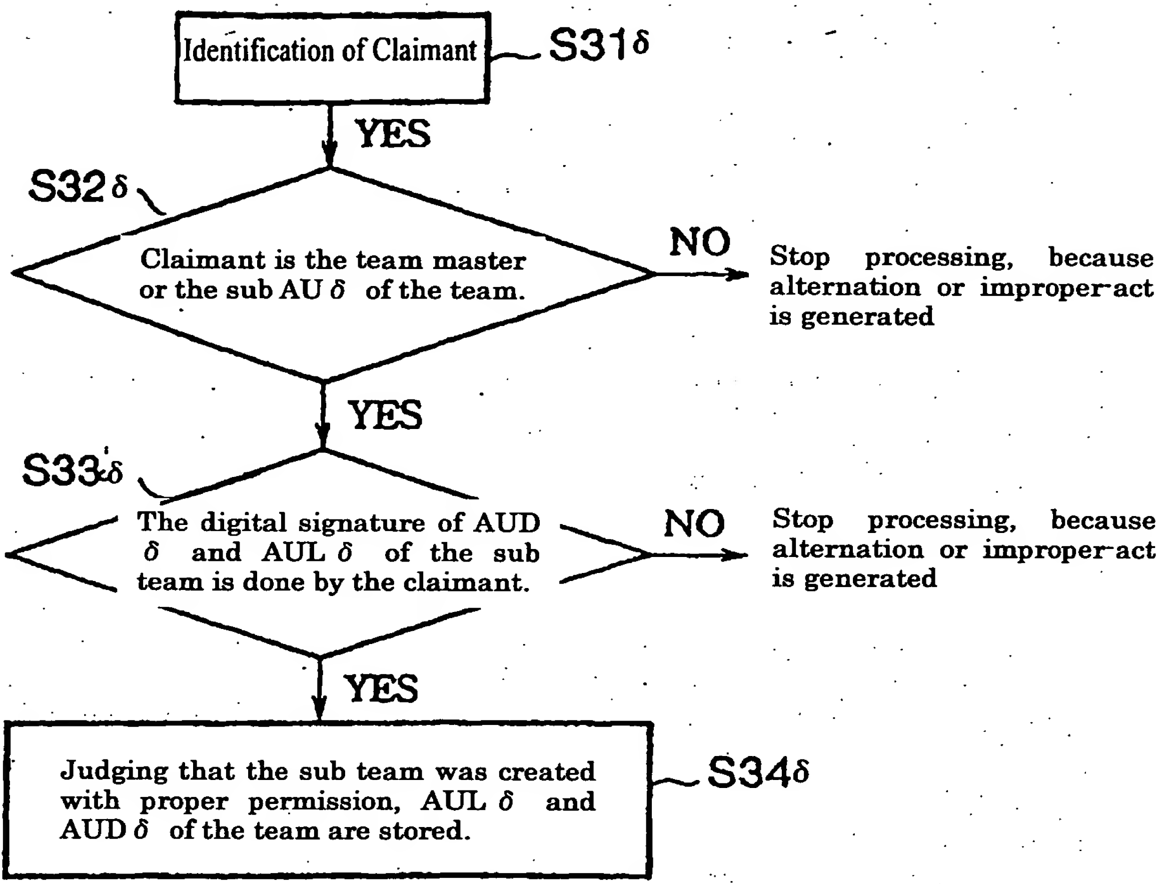

Identification of Claimant
S31δ
YES
S32δ
Claimant is the team master or the sub AU δ of the team.
NO
Stop processing, because alternation or improper-act is generated
YES
S33δ
The digital signature of AUD δ and AUL δ of the sub team is done by the claimant.
NO
Stop processing, because alternation or improper-act is generated
YES
Judging that the sub team was created with proper permission, AUL δ and AUD δ of the team are stored.
S34δ

FIG.43

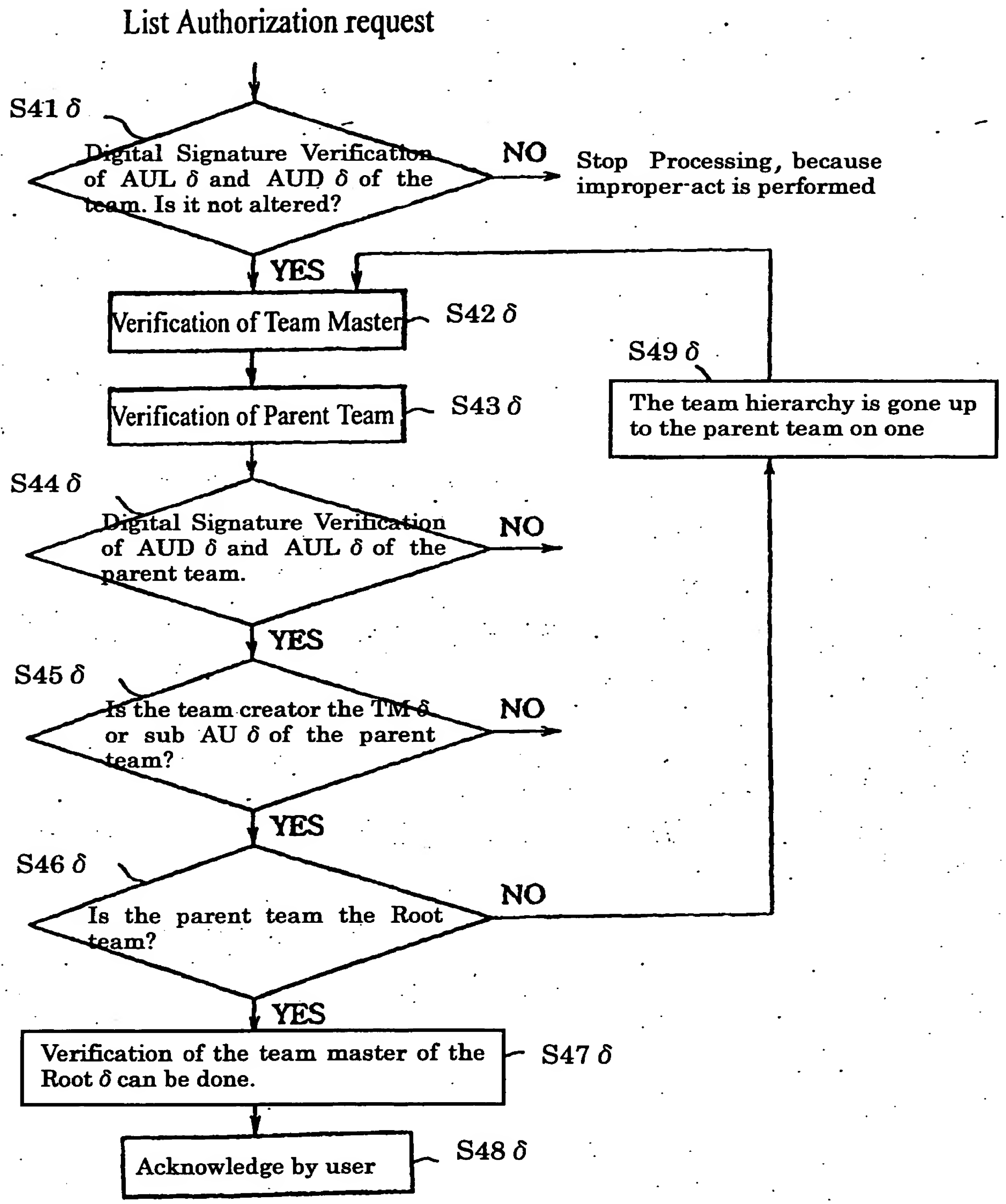

List Authorization request
S41 δ
Digital Signature Verification of AUL δ and AUD δ of the team. Is it not altered?
NO
Stop Processing, because improper act is performed
YES
Verification of Team Master
S42 δ
Verification of Parent Team
S43 δ
S49 δ
The team hierarchy is gone up to the parent team on one
S44 δ
Digital Signature Verification of AUD δ and AUL δ of the parent team.
NO
YES
S45 δ
Is the team creator the TM δ or sub AU δ of the parent team?
NO
YES
S46 δ
Is the parent team the Root team?
NO
YES
Verification of the team master of the Root δ can be done.
S47 δ
Acknowledge by user
S48 δ

FIG.44

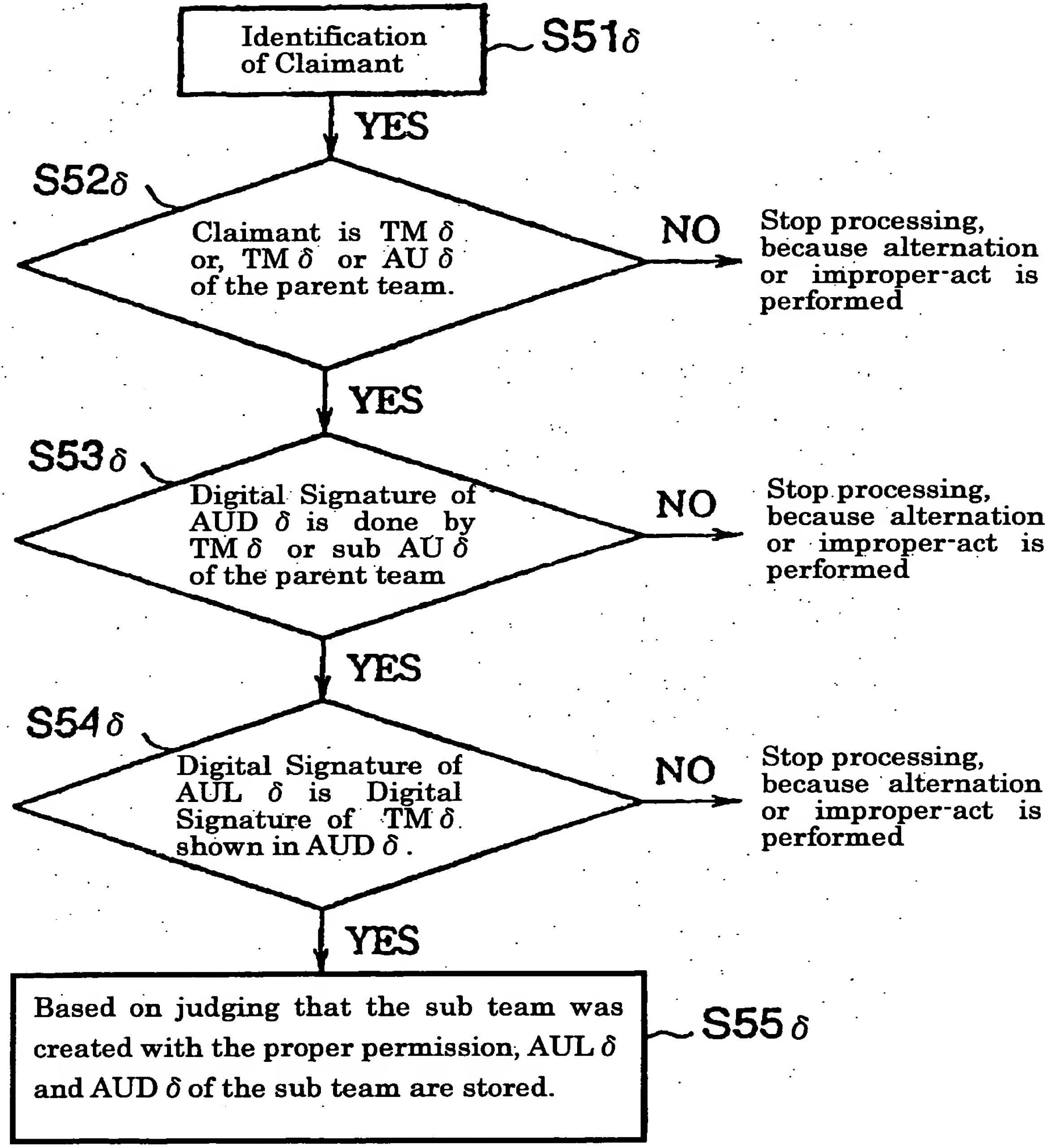

Identification of Claimant
S51δ
YES
S52δ
Claimant is TM δ or, TM δ or AU δ of the parent team.
NO
Stop processing, because alternation or improper-act is performed
YES
S53δ
Digital Signature of AUD δ is done by TM δ or sub AU δ of the parent team
NO
Stop processing, because alternation or improper-act is performed
YES
S54δ
Digital Signature of AUL δ is Digital Signature of TM δ shown in AUD δ .
NO
Stop processing, because alternation or improper-act is performed
YES
Based on judging that the sub team was created with the proper permission, AUL δ and AUD δ of the sub team are stored.
S55δ

FIG.45

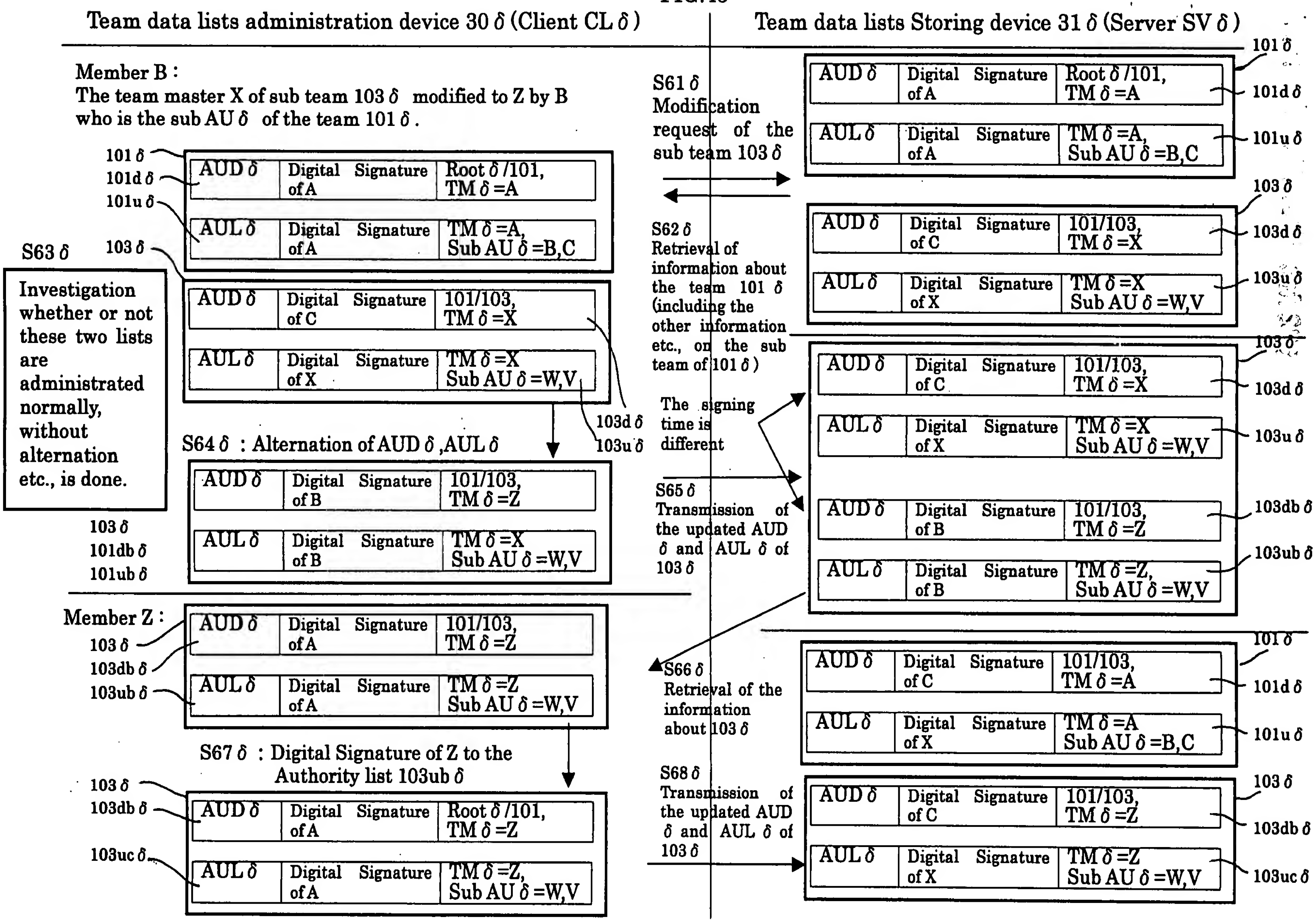

Team data lists administration device 30 δ (Client CL δ)
Team data lists Storing device 31 δ (Server SV δ)
Member B :
The team master X of sub team 103 δ modified to Z by B who is the sub AU δ of the team 101 δ .
101 δ
101d δ
101u δ
103 δ
AUD δ
Digital Signature of A
Root δ /101, TM δ =A
AUL δ
Digital Signature of A
TM δ =A, Sub AU δ =B,C
AUD δ
Digital Signature of C
101/103, TM δ =X
AUL δ
Digital Signature of X
TM δ =X Sub AU δ =W,V
S63 δ
Investigation whether or not these two lists are administrated normally, without alternation etc., is done.
103d δ
103u δ
S64 δ : Alternation of AUD δ ,AUL δ
AUD δ
Digital Signature of B
101/103, TM δ =Z
AUL δ
Digital Signature of B
TM δ =X Sub AU δ =W,V
103 δ
101db δ
101ub δ
Member Z :
103 δ
103db δ
103ub δ
AUD δ
Digital Signature of A
101/103, TM δ =Z
AUL δ
Digital Signature of A
TM δ =Z Sub AU δ =W,V
S67 δ : Digital Signature of Z to the Authority list 103ub δ
103 δ
103db δ
103uc δ
AUD δ
Digital Signature of A
Root δ /101, TM δ =Z
AUL δ
Digital Signature of A
TM δ =Z, Sub AU δ =W,V
S61 δ Modification request of the sub team 103 δ
S62 δ Retrieval of information about the team 101 δ (including the other information etc., on the sub team of 101 δ)
The signing time is different
S65 δ Transmission of the updated AUD δ and AUL δ of 103 δ
S66 δ Retrieval of the information about 103 δ
S68 δ Transmission of the updated AUD δ and AUL δ of 103 δ
101 δ
101d δ
101u δ
AUD δ
Digital Signature of A
Root δ /101, TM δ =A
AUL δ
Digital Signature of A
TM δ =A, Sub AU δ =B,C
103 δ
103d δ
103u δ
AUD δ
Digital Signature of C
101/103, TM δ =X
AUL δ
Digital Signature of X
TM δ =X Sub AU δ =W,V
103 δ
103d δ
103u δ
103db δ
103ub δ
AUD δ
Digital Signature of C
101/103, TM δ =X
AUL δ
Digital Signature of X
TM δ =X Sub AU δ =W,V
AUD δ
Digital Signature of B
101/103, TM δ =Z
AUL δ
Digital Signature of B
TM δ =Z, Sub AU δ =W,V
101 δ
101d δ
101u δ
AUD δ
Digital Signature of C
101/103, TM δ =A
AUL δ
Digital Signature of X
TM δ =A Sub AU δ =B,C
103 δ
103db δ
103uc δ
AUD δ
Digital Signature of C
101/103, TM δ =Z
AUL δ
Digital Signature of X
TM δ =Z Sub AU δ =W,V

FIG.46

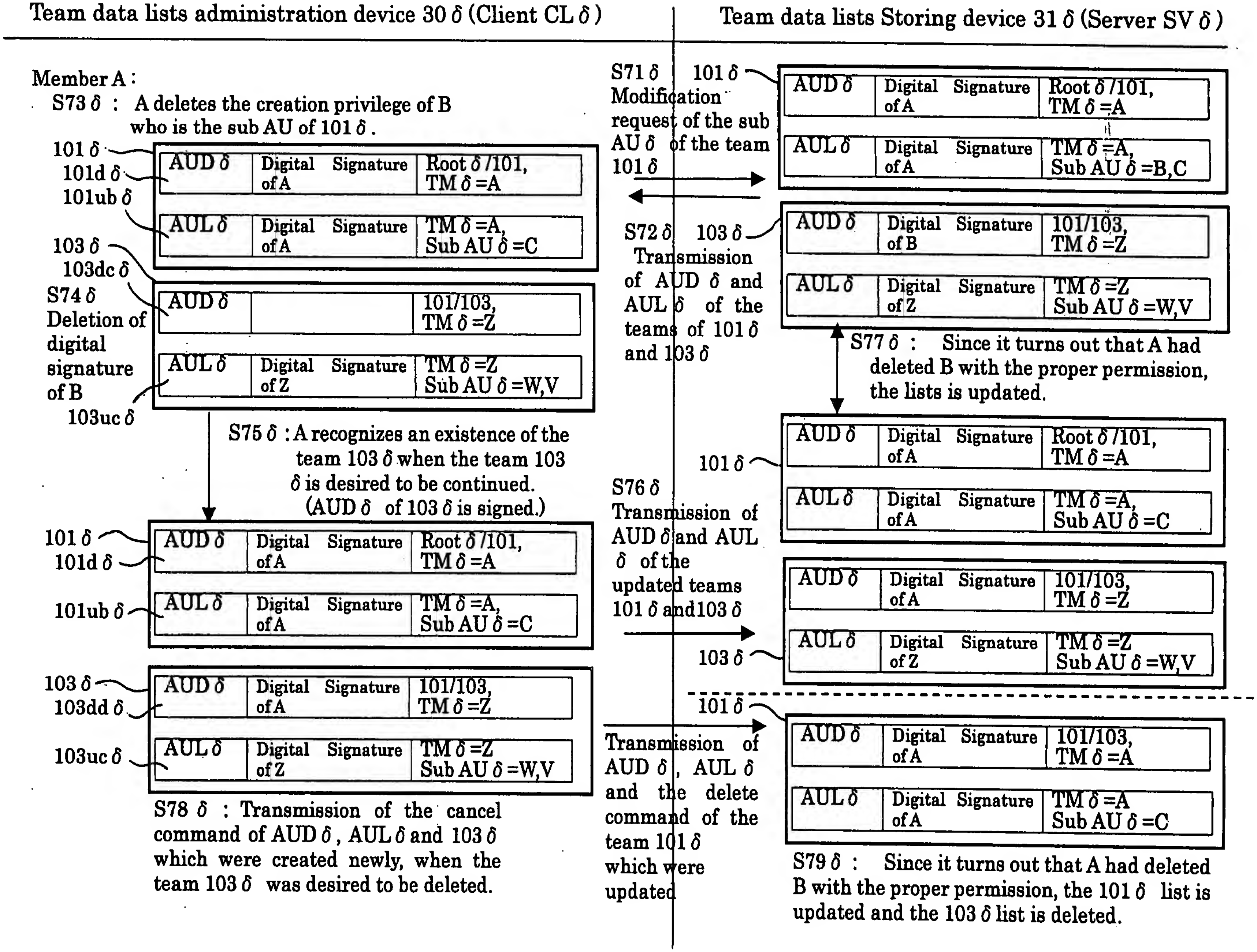
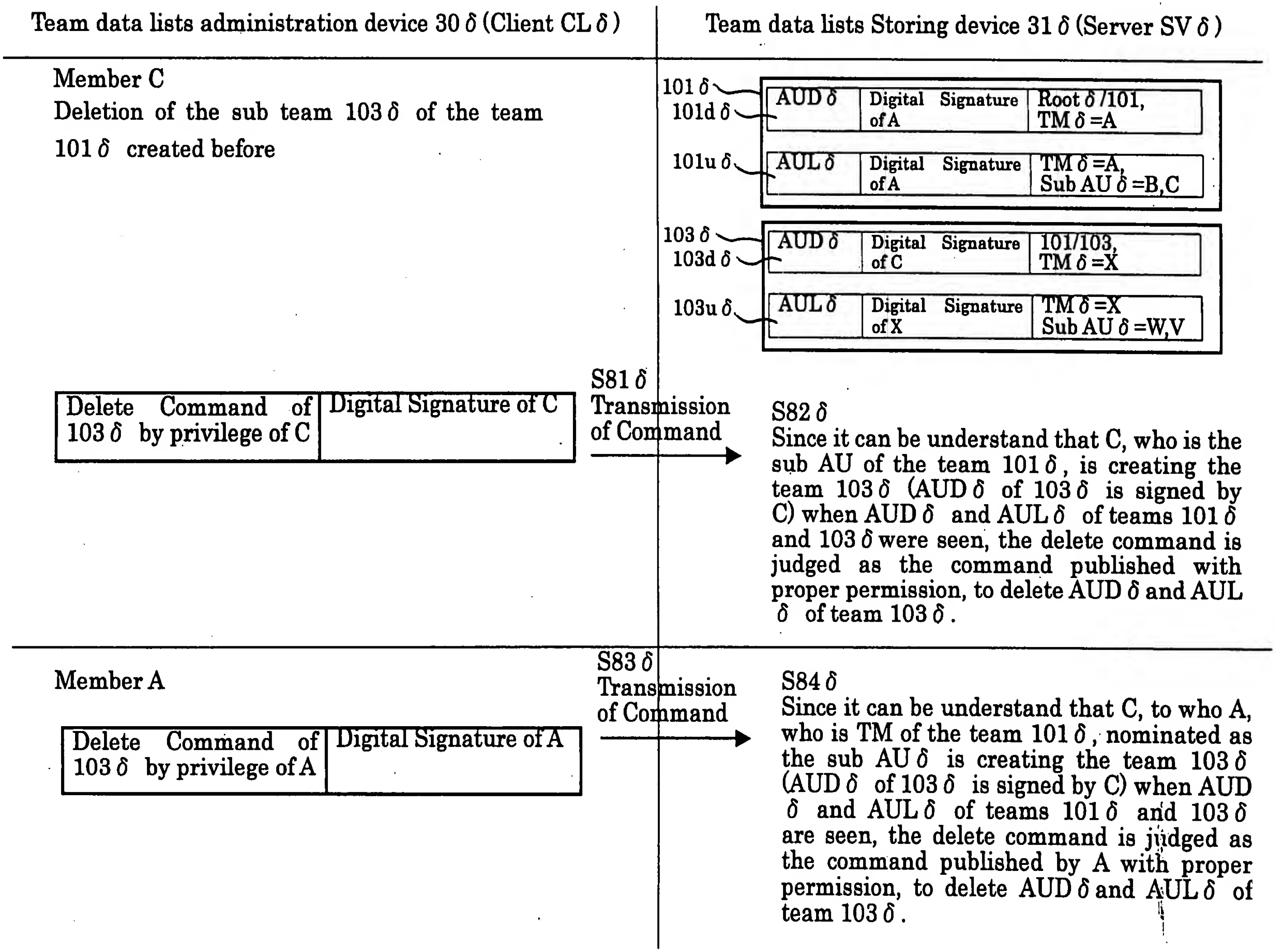

Team data lists administration device 30δ (Client CLδ)
Team data lists Storing device 31δ (Server SVδ)
Member A :
S73δ : A deletes the creation privilege of B who is the sub AU of 101δ .
101δ
101dδ
101ubδ
AUDδ
Digital Signature of A
Root δ/101, TMδ =A
AULδ
Digital Signature of A
TMδ =A, Sub AUδ =C
103δ
103dcδ
S74δ Deletion of digital signature of B
AUDδ
101/103, TMδ =Z
AULδ
Digital Signature of Z
TMδ =Z Sub AUδ =W,V
103ucδ
S75δ : A recognizes an existence of the team 103δ when the team 103 δ is desired to be continued. (AUDδ of 103δ is signed.)
101δ
101dδ
AUDδ
Digital Signature of A
Root δ/101, TMδ =A
101ubδ
AULδ
Digital Signature of A
TMδ =A, Sub AUδ =C
103δ
103ddδ
AUDδ
Digital Signature of A
101/103, TMδ =Z
103ucδ
AULδ
Digital Signature of Z
TMδ =Z Sub AUδ =W,V
S78δ : Transmission of the cancel command of AUDδ, AULδ and 103δ which were created newly, when the team 103δ was desired to be deleted.
S71δ Modification request of the sub AUδ of the team 101δ
101δ
AUDδ
Digital Signature of A
Root δ/101, TMδ =A
AULδ
Digital Signature of A
TMδ =A, Sub AUδ =B,C
S72δ Transmission of AUDδ and AULδ of the teams of 101δ and 103δ
103δ
AUDδ
Digital Signature of B
101/103, TMδ =Z
AULδ
Digital Signature of Z
TMδ =Z Sub AUδ =W,V
S77δ : Since it turns out that A had deleted B with the proper permission, the lists is updated.
101δ
AUDδ
Digital Signature of A
Root δ/101, TMδ =A
AULδ
Digital Signature of A
TMδ =A, Sub AUδ =C
S76δ Transmission of AUDδ and AUL δ of the updated teams 101δ and103δ
103δ
AUDδ
Digital Signature of A
101/103, TMδ =Z
AULδ
Digital Signature of Z
TMδ =Z Sub AUδ =W,V
101δ
Transmission of AUDδ, AULδ and the delete command of the team 101δ which were updated
AUDδ
Digital Signature of A
101/103, TMδ =A
AULδ
Digital Signature of A
TMδ =A Sub AUδ =C
S79δ : Since it turns out that A had deleted B with the proper permission, the 101δ list is updated and the 103δ list is deleted.

FIG.47



Team data lists administration device 30δ (Client CLδ)

Team data lists Storing device 31δ (Server SVδ)

Member C
Deletion of the sub team 103δ of the team 101δ created before

AUDδ	Digital Signature of A	Rootδ/101, TMδ=A
AULδ	Digital Signature of A	TMδ=A, Sub AUδ=B,C

AUDδ	Digital Signature of C	101/103, TMδ=X
AULδ	Digital Signature of X	TMδ=X Sub AUδ=W,V

Delete Command of 103δ by privilege of C	Digital Signature of C

S81δ Transmission of Command

S82δ
Since it can be understand that C, who is the sub AU of the team 101δ, is creating the team 103δ (AUDδ of 103δ is signed by C) when AUDδ and AULδ of teams 101δ and 103δ were seen, the delete command is judged as the command published with proper permission, to delete AUDδ and AULδ of team 103δ.

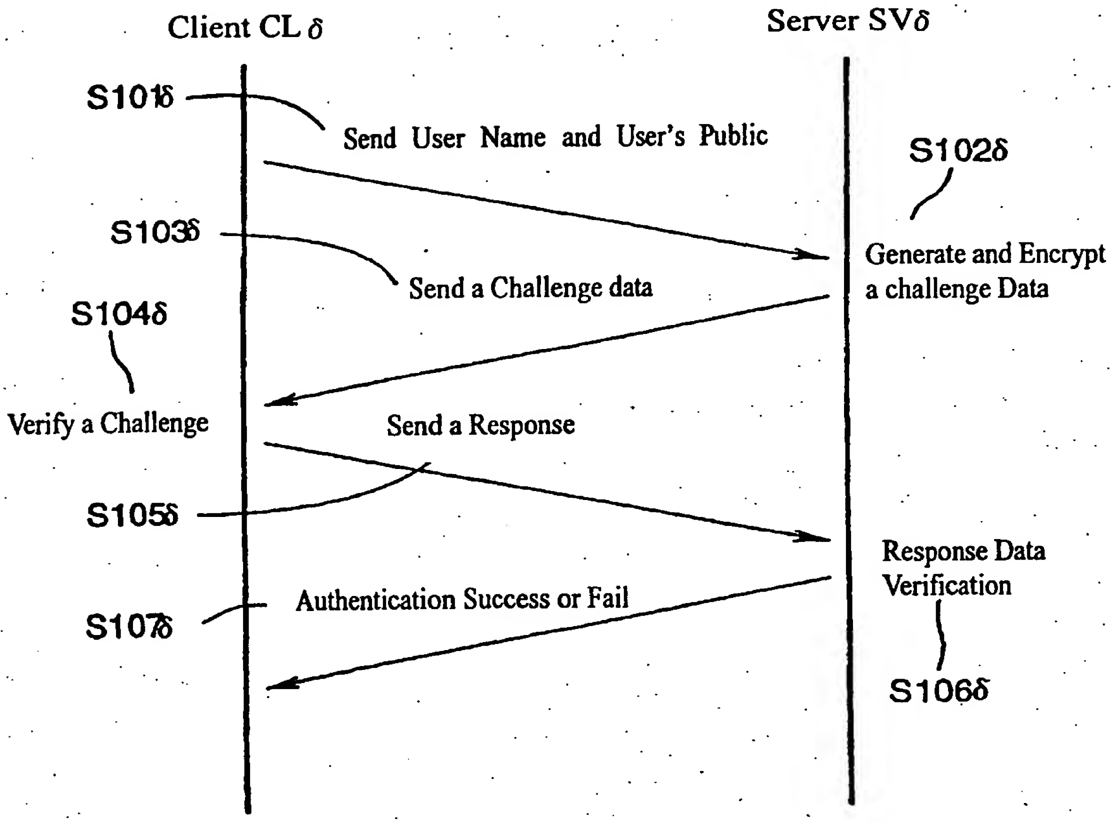
Member A

Delete Command of 103δ by privilege of A	Digital Signature of A

S83δ Transmission of Command

S84δ
Since it can be understand that C, to who A, who is TM of the team 101δ, nominated as the sub AUδ is creating the team 103δ (AUDδ of 103δ is signed by C) when AUDδ and AULδ of teams 101δ and 103δ are seen, the delete command is judged as the command published by A with proper permission, to delete AUDδ and AULδ of team 103δ.

FIG.48


Client CL δ
Server SVδ
S101δ
Send User Name and User's Public
S102δ
Generate and Encrypt a challenge Data
S103δ
Send a Challenge data
S104δ
Verify a Challenge
Send a Response
S105δ
Response Data Verification
S106δ
Authentication Success or Fail
S107δ

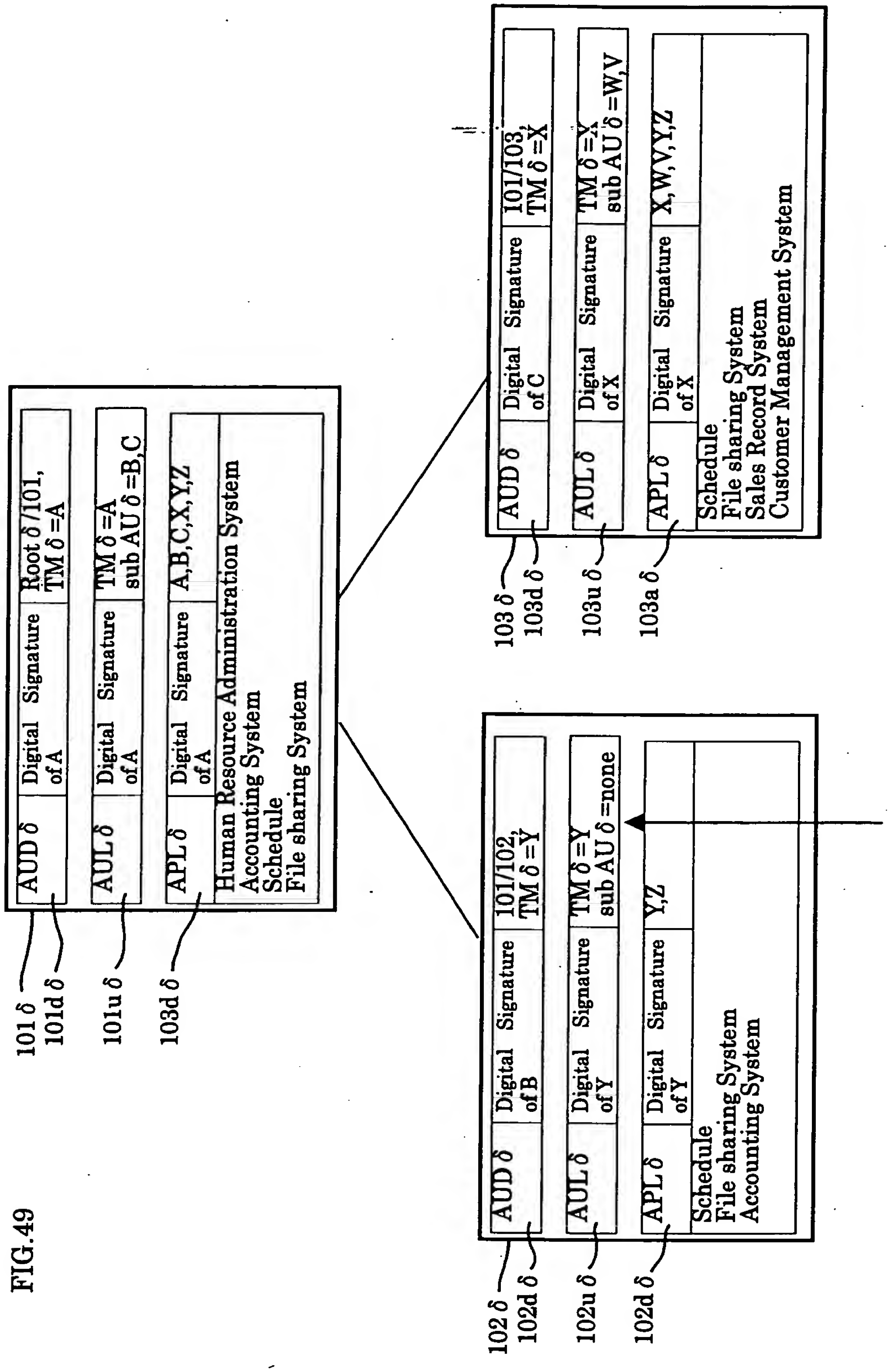
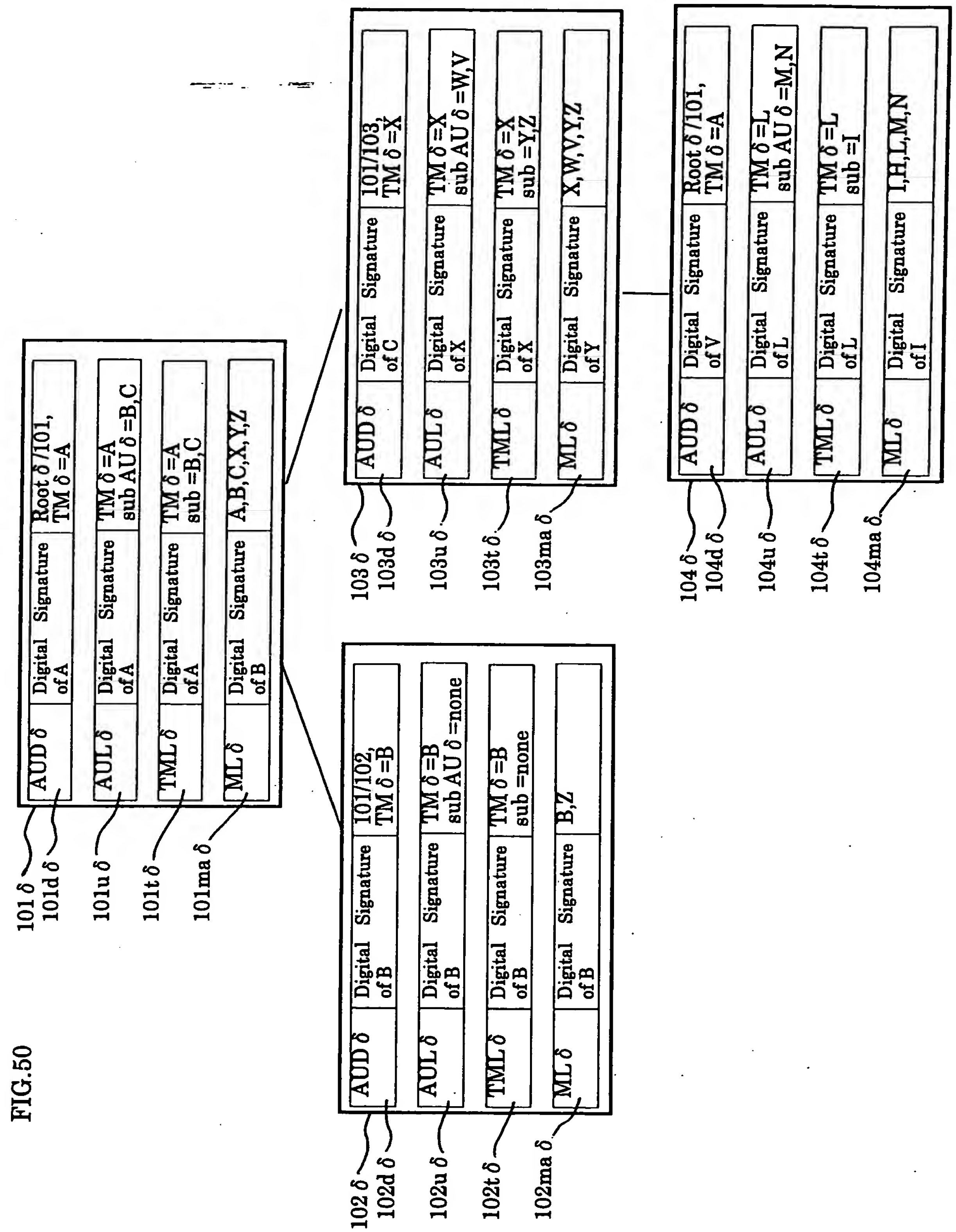

AUD δ
Digital Signature of A
Root δ /101, TM δ =A
AUL δ
Digital Signature of A
TM δ =A sub AU δ =B,C
APL δ
Digital Signature of A
A,B,C,X,Y,Z
Human Resource Administration System
Accounting System
Schedule
File sharing System
101 δ
101d δ
101u δ
103d δ
AUD δ
Digital Signature of B
101/102, TM δ =Y
AUL δ
Digital Signature of Y
TM δ =Y sub AU δ =none
APL δ
Digital Signature of Y
Y,Z
Schedule
File sharing System
Accounting System
102 δ
102d δ
102u δ
102d δ
AUD δ
Digital Signature of C
101/103, TM δ =X
AUL δ
Digital Signature of X
TM δ =X sub AU δ =W,V
APL δ
Digital Signature of X
X,W,V,Y,Z
Schedule
File sharing System
Sales Record System
Customer Management System
103 δ
103d δ
103u δ
103a δ

FIG.49

FIG.50


AUD δ
Digital of A
Signature
Root δ/101, TM δ =A
AUL δ
Digital of A
Signature
TM δ =A sub AU δ =B,C
TML δ
Digital of A
Signature
TM δ =A sub =B,C
ML δ
Digital of B
Signature
A,B,C,X,Y,Z
101 δ
101d δ
101u δ
101t δ
101ma δ
AUD δ
Digital of B
Signature
101/102, TM δ =B
AUL δ
Digital of B
Signature
TM δ =B sub AU δ =none
TML δ
Digital of B
Signature
TM δ =B sub =none
ML δ
Digital of B
Signature
B,Z
102 δ
102d δ
102u δ
102t δ
102ma δ
AUD δ
Digital of C
Signature
101/103, TM δ =X
AUL δ
Digital of X
Signature
TM δ =X sub AU δ =W,V
TML δ
Digital of X
Signature
TM δ =X sub =Y,Z
ML δ
Digital of Y
Signature
X,W,V,Y,,Z
103 δ
103d δ
103u δ
103t δ
103ma δ
AUD δ
Digital of V
Signature
Root δ/101, TM δ =A
AUL δ
Digital of L
Signature
TM δ =L sub AU δ =M,N
TML δ
Digital of L
Signature
TM δ =L sub =I
ML δ
Digital of I
Signature
I,H,L,M,N
104 δ
104d δ
104u δ
104t δ
104ma δ

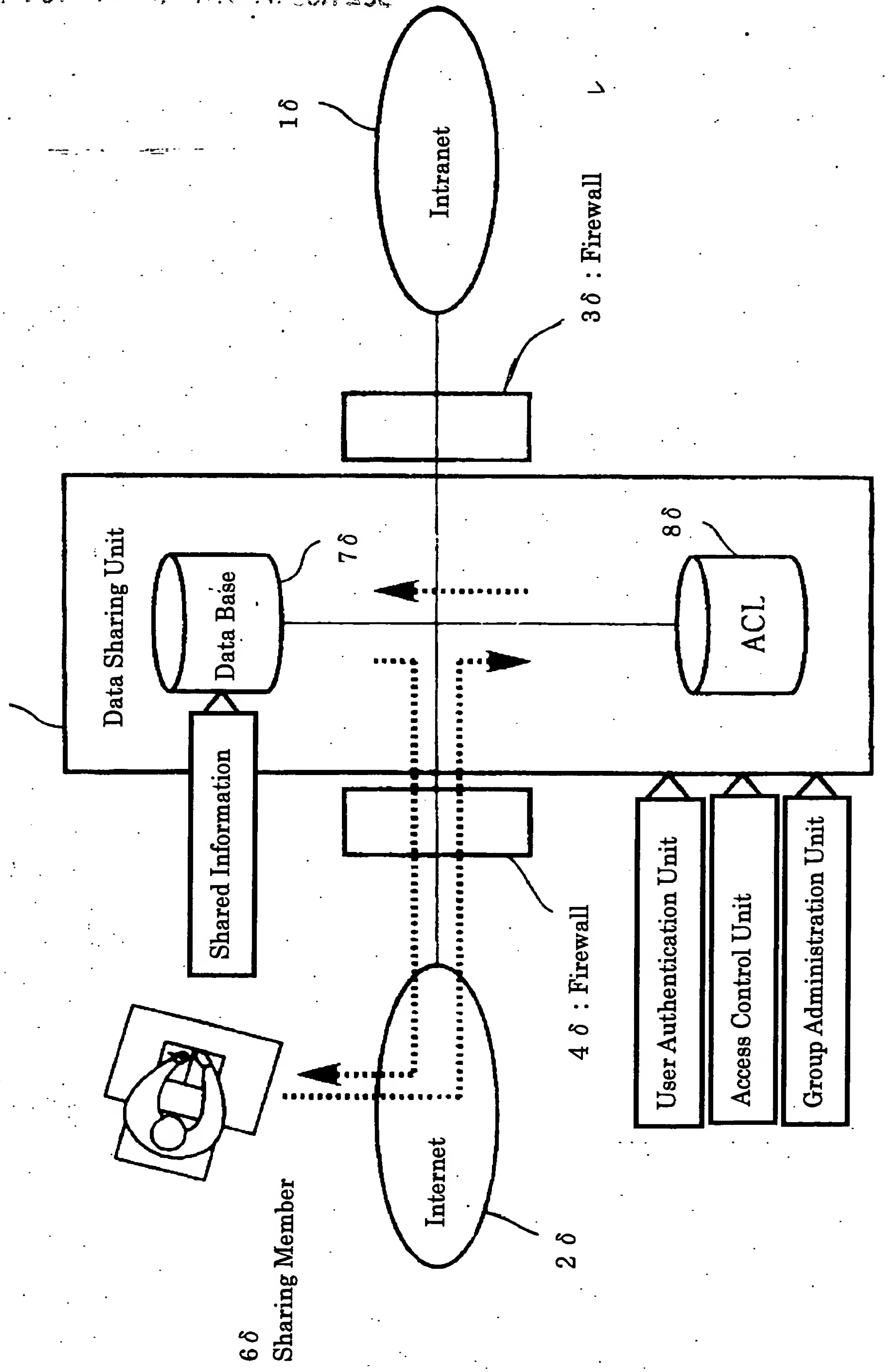

1δ
Intranet
3δ : Firewall
5δ : Server
Data Sharing Unit
Data Base
7δ
8δ
ACL
Shared Information
4δ : Firewall
User Authentication Unit
Access Control Unit
Group Administration Unit
Internet
2δ
6δ
Sharing Member

FIG.51

FIG.52

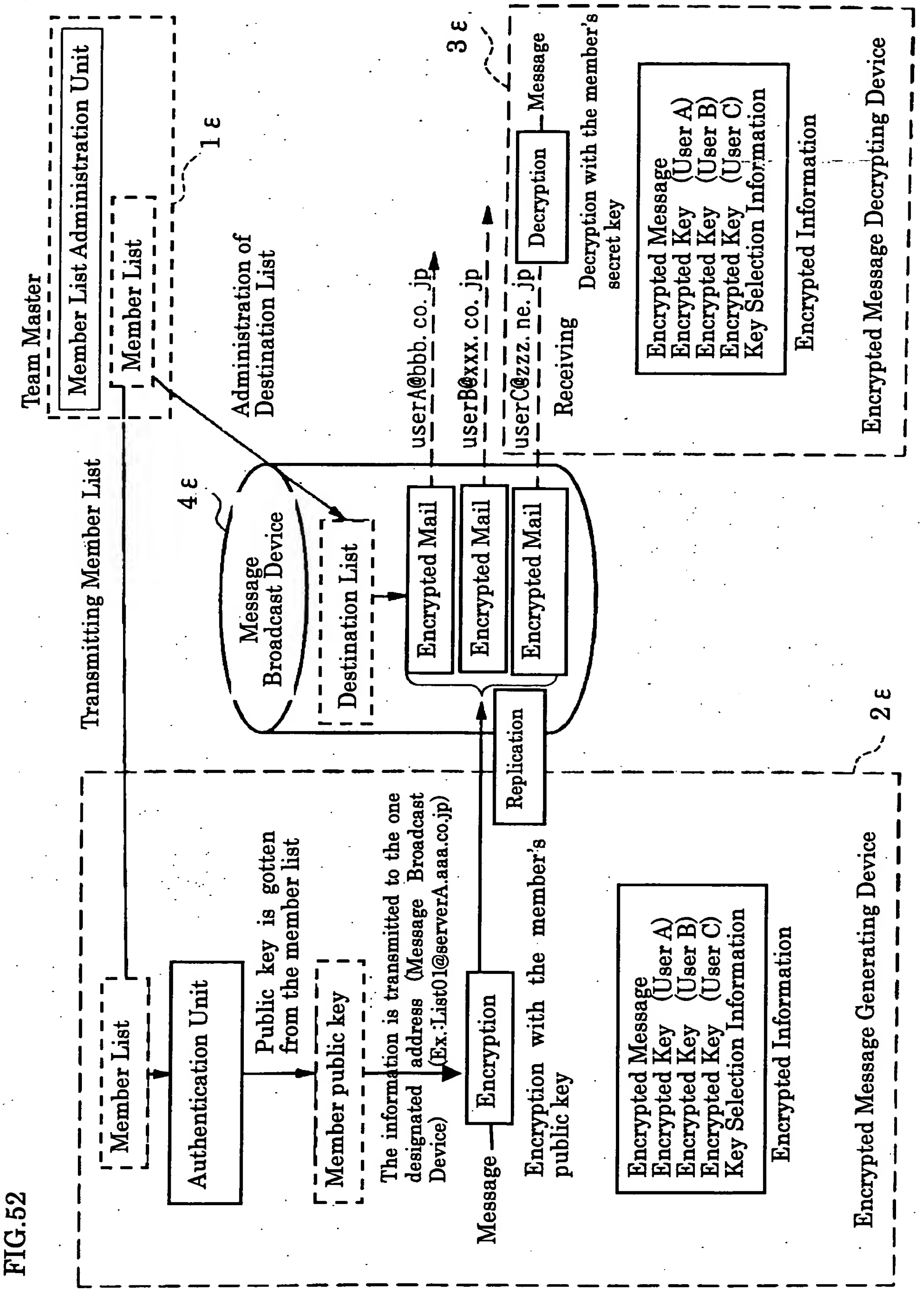
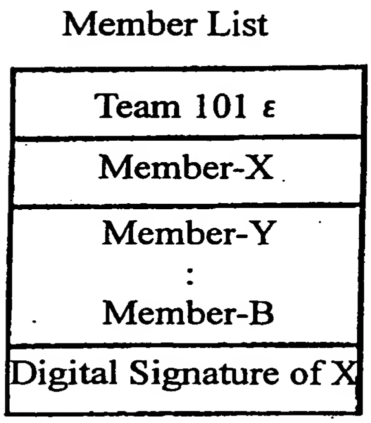

Team Master
Member List Administration Unit
Member List
1 ε
Administration of Destination List
Transmitting Member List
4 ε
Message Broadcast Device
Destination List
Encrypted Mail
Encrypted Mail
Encrypted Mail
Replication
userA@bbb. co. jp
userB@xxx. co. jp
userC@zz. ne. jp
Receiving
3 ε
Decryption
Message
Decryption with the member's secret key
Encrypted Message
Encrypted Key (User A)
Encrypted Key (User B)
Encrypted Key (User C)
Key Selection Information
Encrypted Information
Encrypted Message Decrypting Device
2 ε
Member List
Authentication Unit
Public key is gotten from the member list
Member public key
The information is transmitted to the one designated address (Message Broadcast Device) (Ex.:List01@serverA.aaa.co.jp)
Message
Encryption
Encryption with the member's public key
Encrypted Message
Encrypted Key (User A)
Encrypted Key (User B)
Encrypted Key (User C)
Key Selection Information
Encrypted Information
Encrypted Message Generating Device

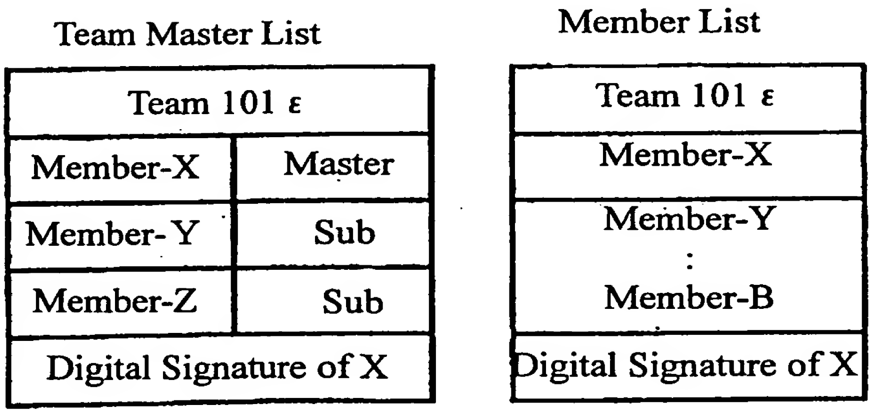
FIG.53



Member List

Team 101 ε
Member-X
Member-Y : Member-B
Digital Signature of X

FIG.54



Team Master List

Team 101 ε	
Member-X	Master
Member-Y	Sub
Member-Z	Sub
Digital Signature of X	

Member List

Team 101 ε
Member-X
Member-Y : Member-B
Digital Signature of X

FIG.55

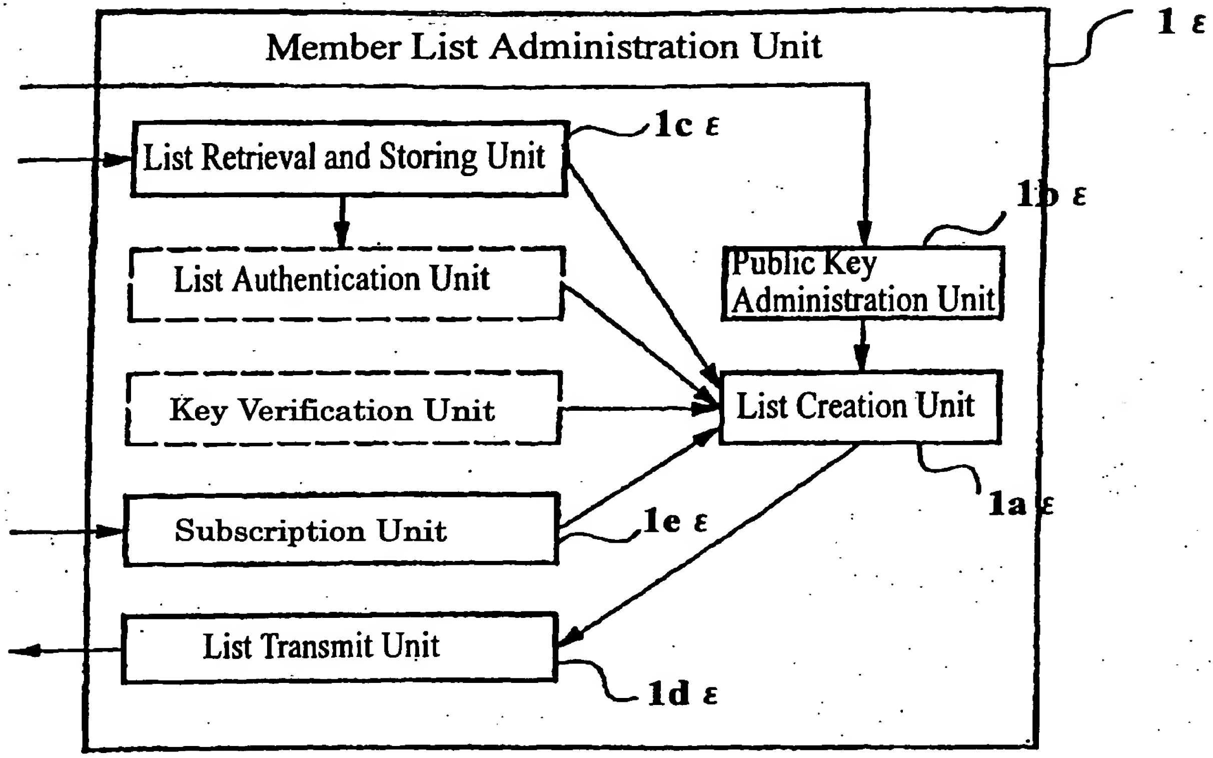

Member List Administration Unit
1 ε
List Retrieval and Storing Unit
1c ε
List Authentication Unit
1b ε
Public Key Administration Unit
Key Verification Unit
List Creation Unit
1a ε
Subscription Unit
1e ε
List Transmit Unit
1d ε

FIG.56

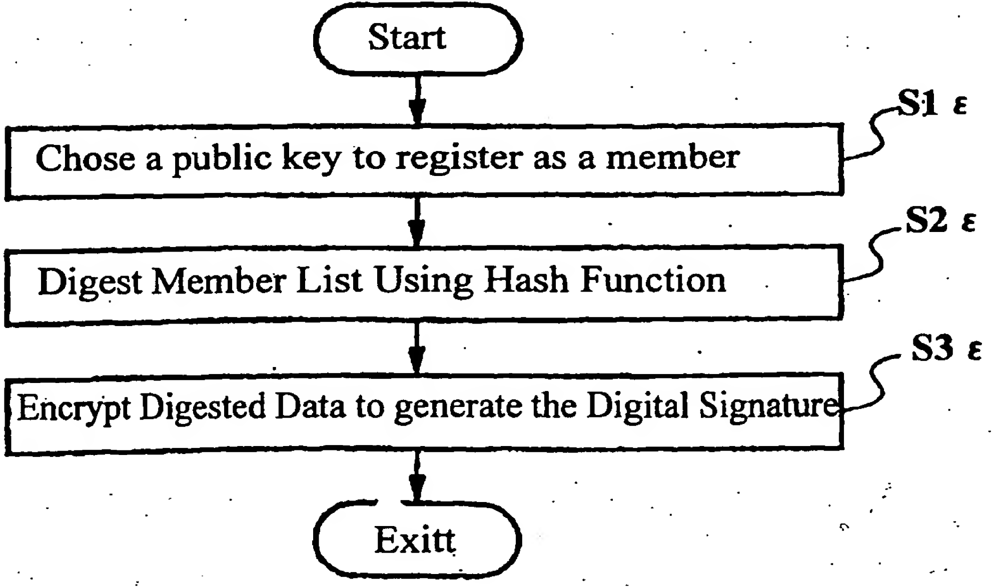

Start
Chose a public key to register as a member
S1 ε
Digest Member List Using Hash Function
S2 ε
Encrypt Digested Data to generate the Digital Signature
S3 ε
Exitt

FIG.57

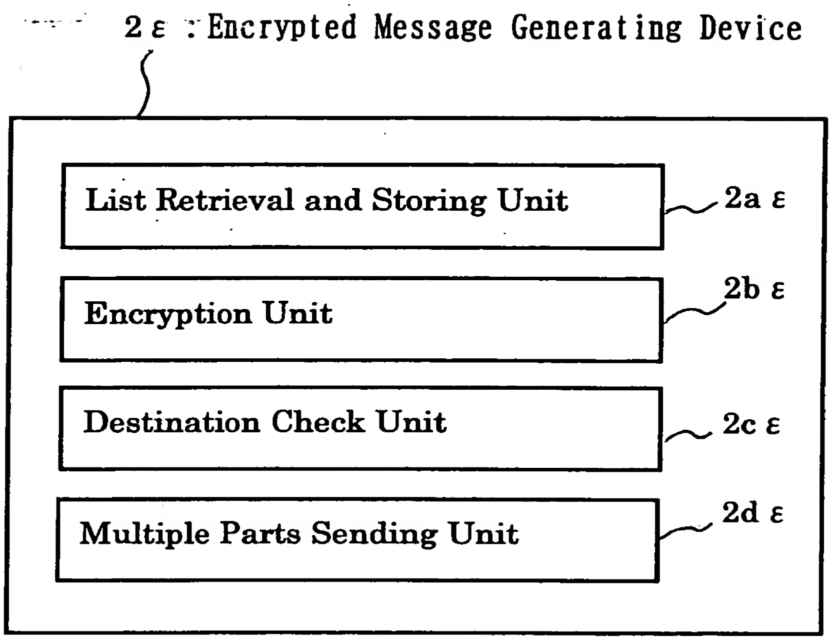

2ε : Encrypted Message Generating Device
List Retrieval and Storing Unit
2a ε
Encryption Unit
2b ε
Destination Check Unit
2c ε
Multiple Parts Sending Unit
2d ε

FIG.58

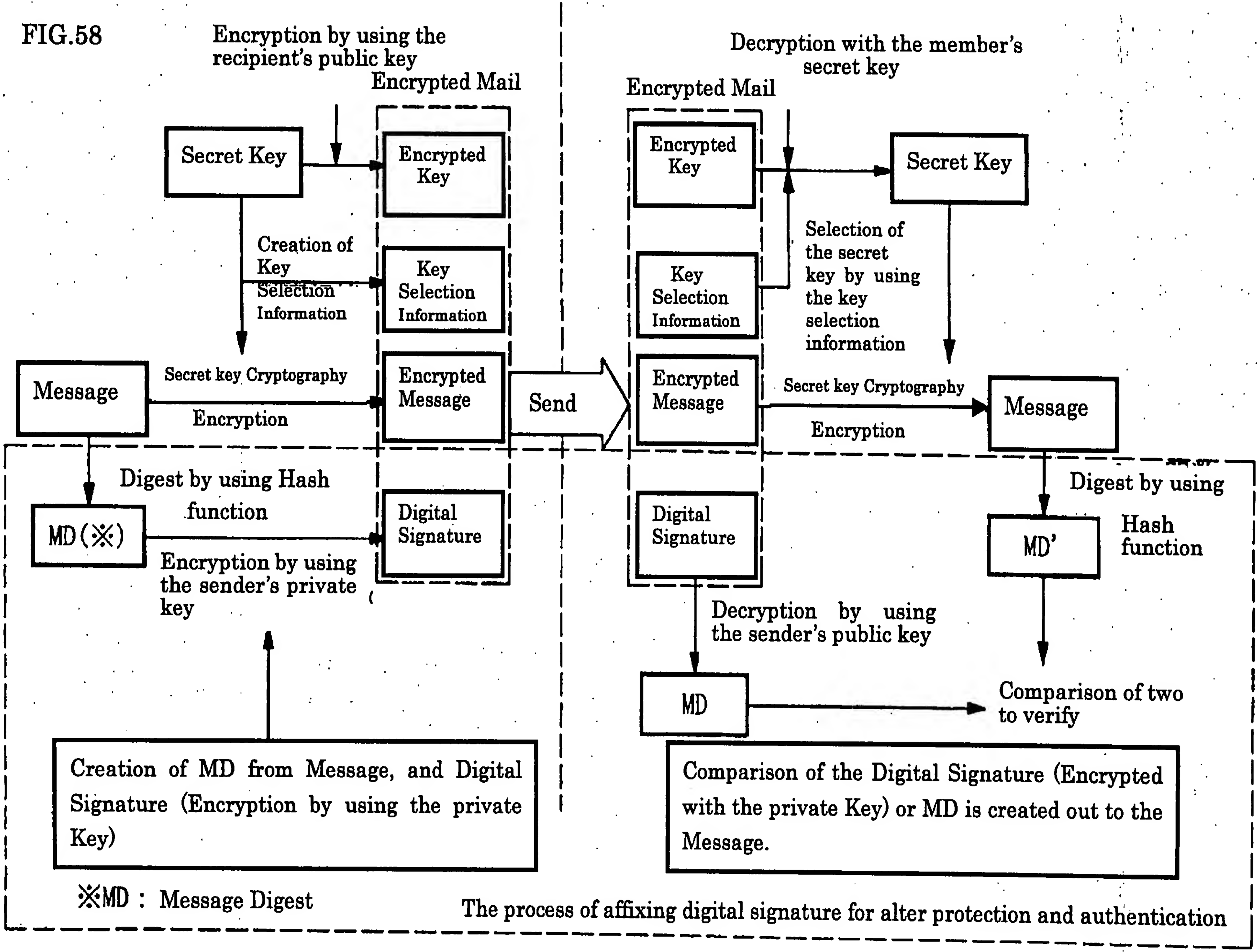

Encryption by using the recipient's public key
Encrypted Mail
Secret Key
Encrypted Key
Creation of Key Selection Information
Key Selection Information
Message
Secret key Cryptography
Encryption
Encrypted Message
Send
Digest by using Hash function
MD(※)
Encryption by using the sender's private key
Digital Signature
Creation of MD from Message, and Digital Signature (Encryption by using the private Key)
※MD : Message Digest
Decryption with the member's secret key
Encrypted Mail
Encrypted Key
Secret Key
Key Selection Information
Selection of the secret key by using the key selection information
Encrypted Message
Secret key Cryptography
Encryption
Message
Digest by using Hash function
MD'
Digital Signature
Decryption by using the sender's public key
MD
Comparison of two to verify
Comparison of the Digital Signature (Encrypted with the private Key) or MD is created out to the Message.
The process of affixing digital signature for alter protection and authentication

FIG.59

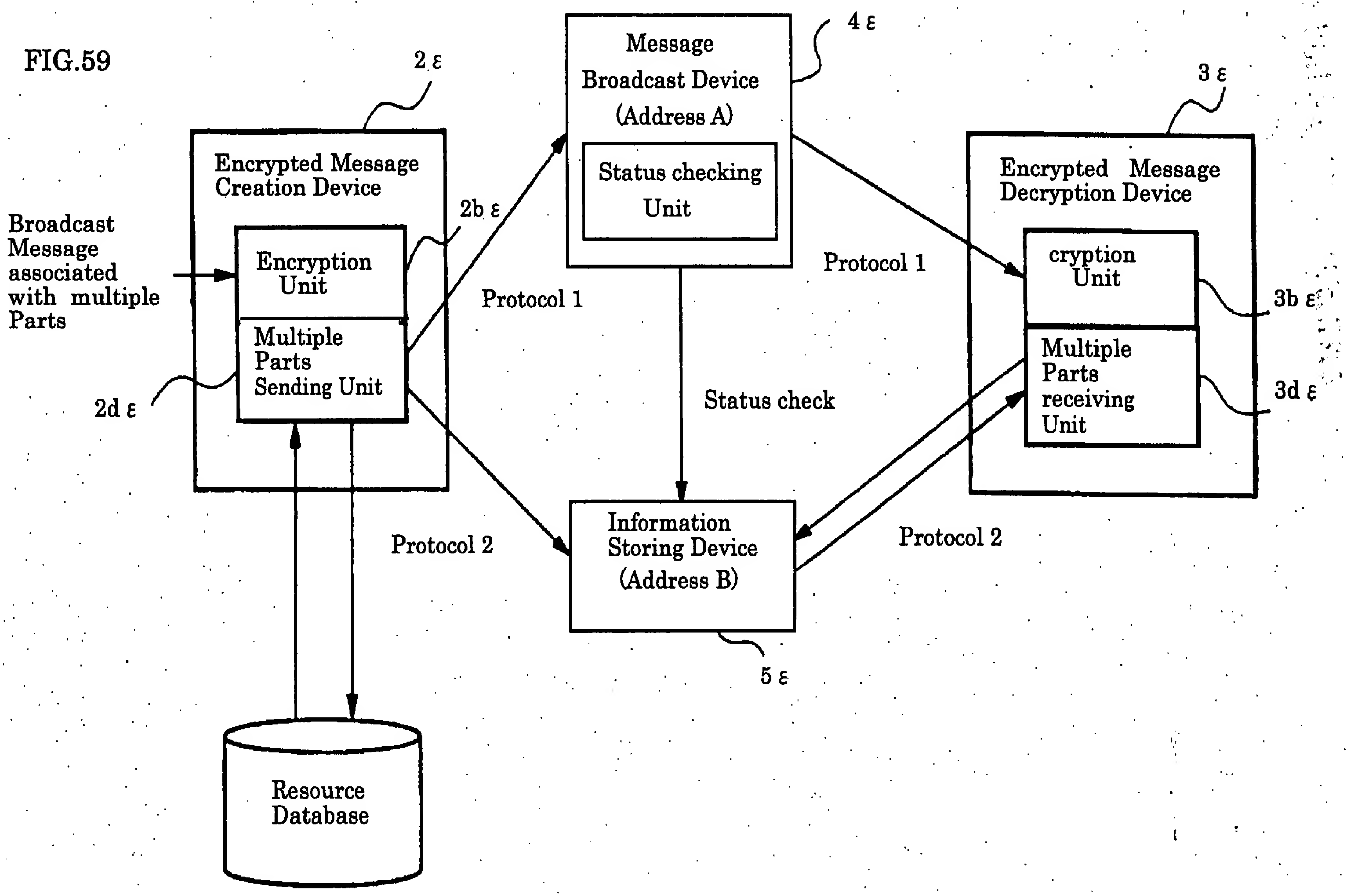

2 ε
Encrypted Message Creation Device
Encryption Unit
Multiple Parts Sending Unit
2b ε
2d ε
Broadcast Message associated with multiple Parts
Resource Database
Protocol 1
Protocol 2
4 ε
Message Broadcast Device (Address A)
Status checking Unit
Status check
Information Storing Device (Address B)
5 ε
Protocol 1
Protocol 2
3 ε
Encrypted Message Decryption Device
cryption Unit
Multiple Parts receiving Unit
3b ε
3d ε

FIG.60

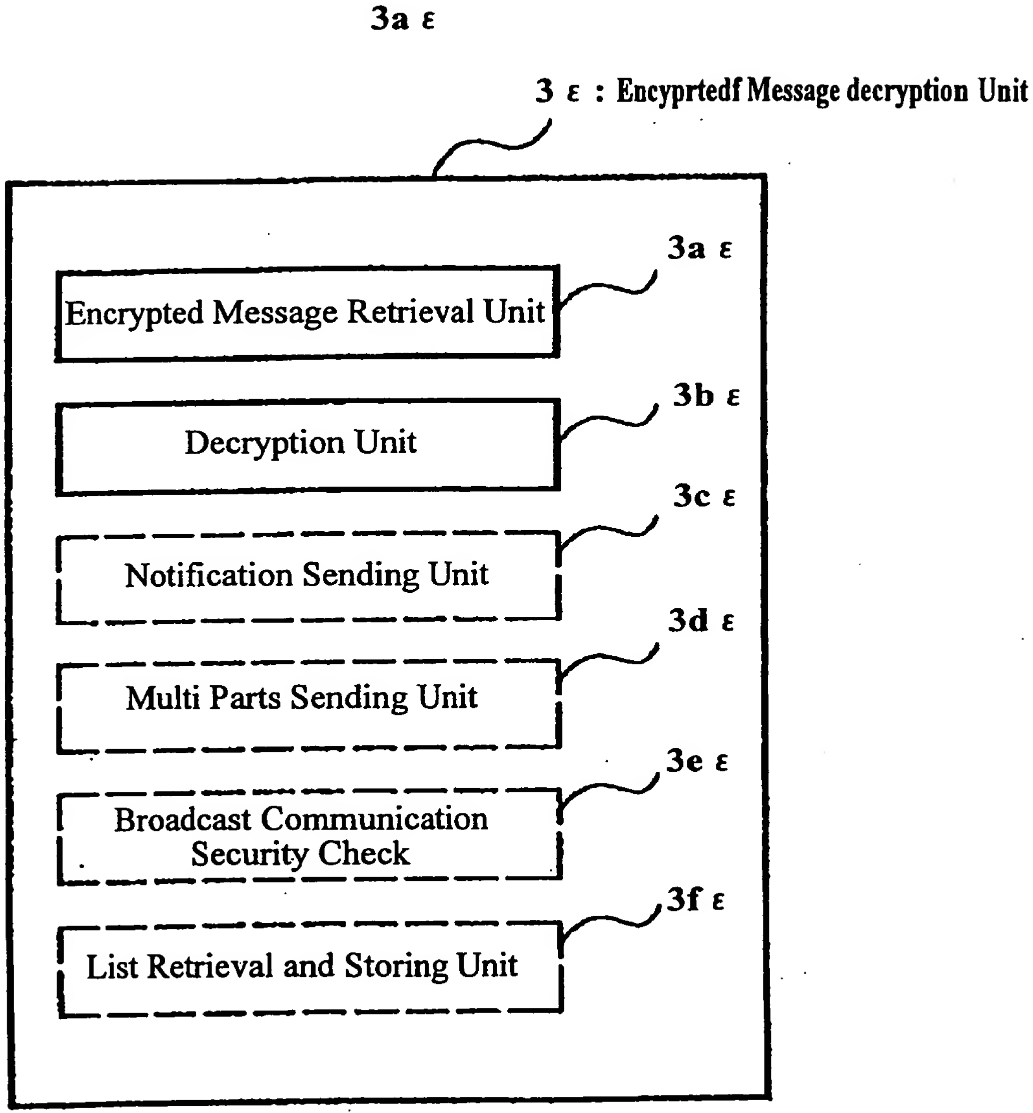

3a ε
3 ε : Encyprtedf Message decryption Unit
3a ε
Encrypted Message Retrieval Unit
3b ε
Decryption Unit
3c ε
Notification Sending Unit
3d ε
Multi Parts Sending Unit
3e ε
Broadcast Communication Security Check
3f ε
List Retrieval and Storing Unit

FIG.61

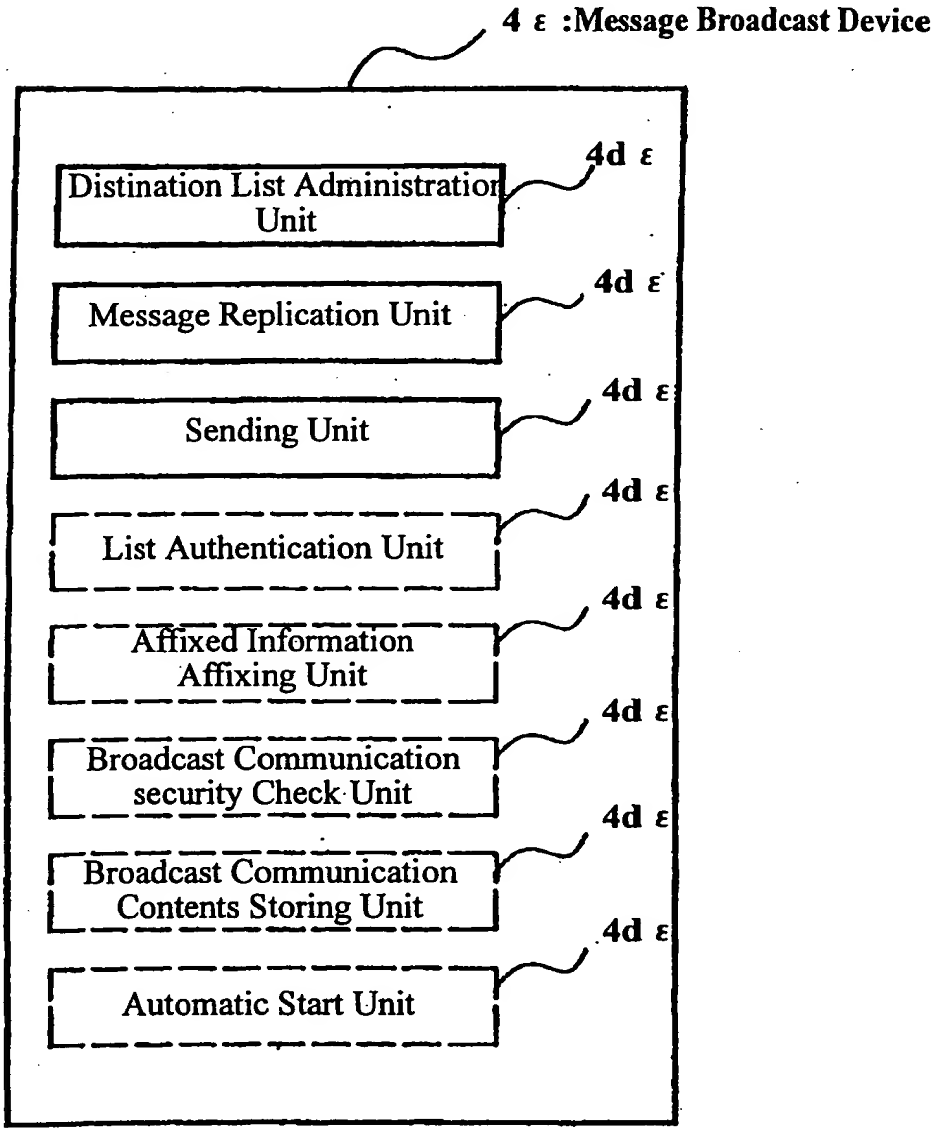

4 ε :Message Broadcast Device
Distination List Administration Unit
4d ε
Message Replication Unit
4d ε
Sending Unit
4d ε
List Authentication Unit
4d ε
Affixed Information Affixing Unit
4d ε
Broadcast Communication security Check Unit
4d ε
Broadcast Communication Contents Storing Unit
4d ε
Automatic Start Unit
4d ε

FIG.62

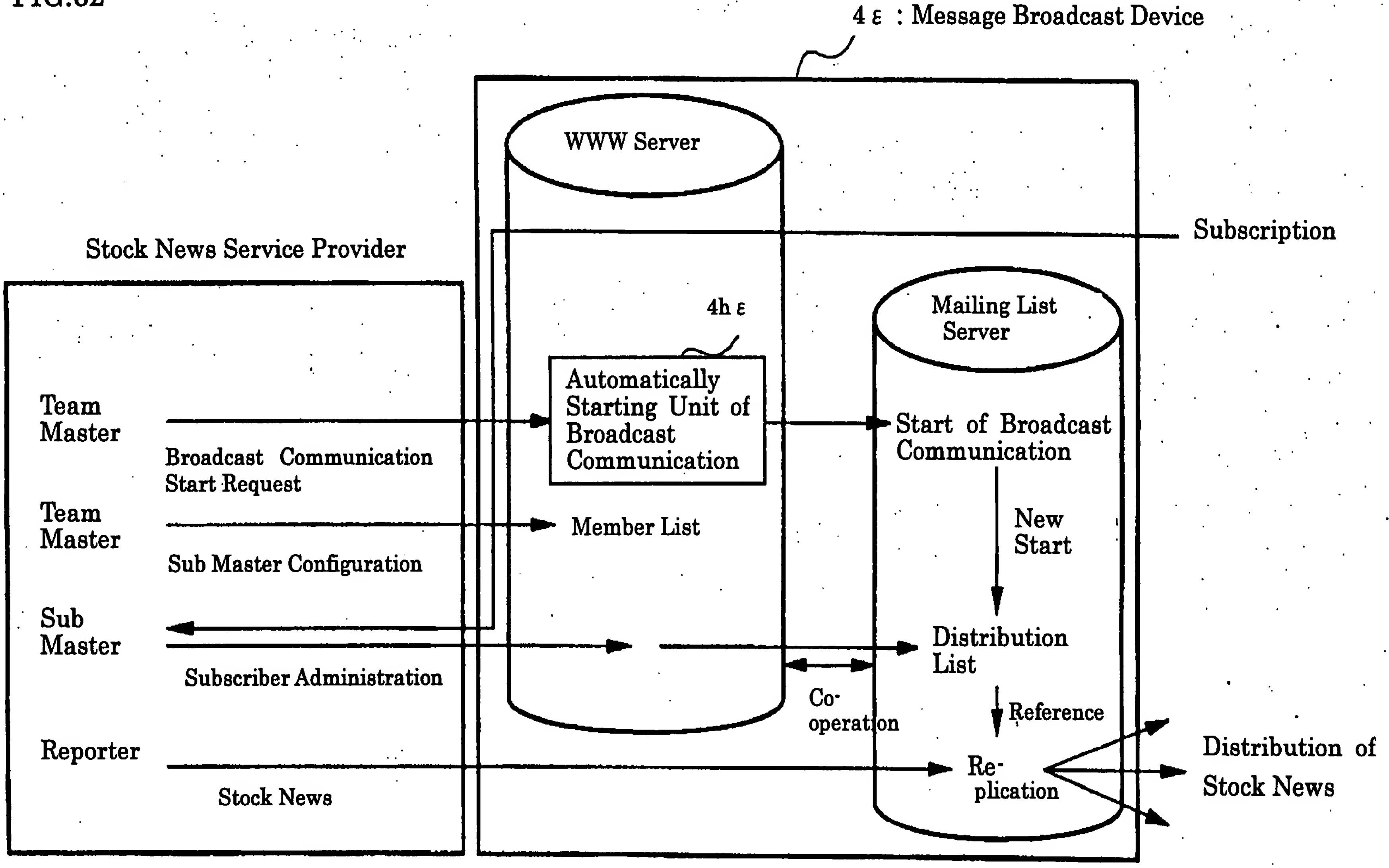

4ε : Message Broadcast Device
Stock News Service Provider
Team Master
Broadcast Communication Start Request
Team Master
Sub Master Configuration
Sub Master
Subscriber Administration
Reporter
Stock News
WWW Server
4hε
Automatically Starting Unit of Broadcast Communication
Member List
Subscription
Mailing List Server
Start of Broadcast Communication
New Start
Distribution List
Co-operation
Reference
Re-plication
Distribution of Stock News

FIG.63

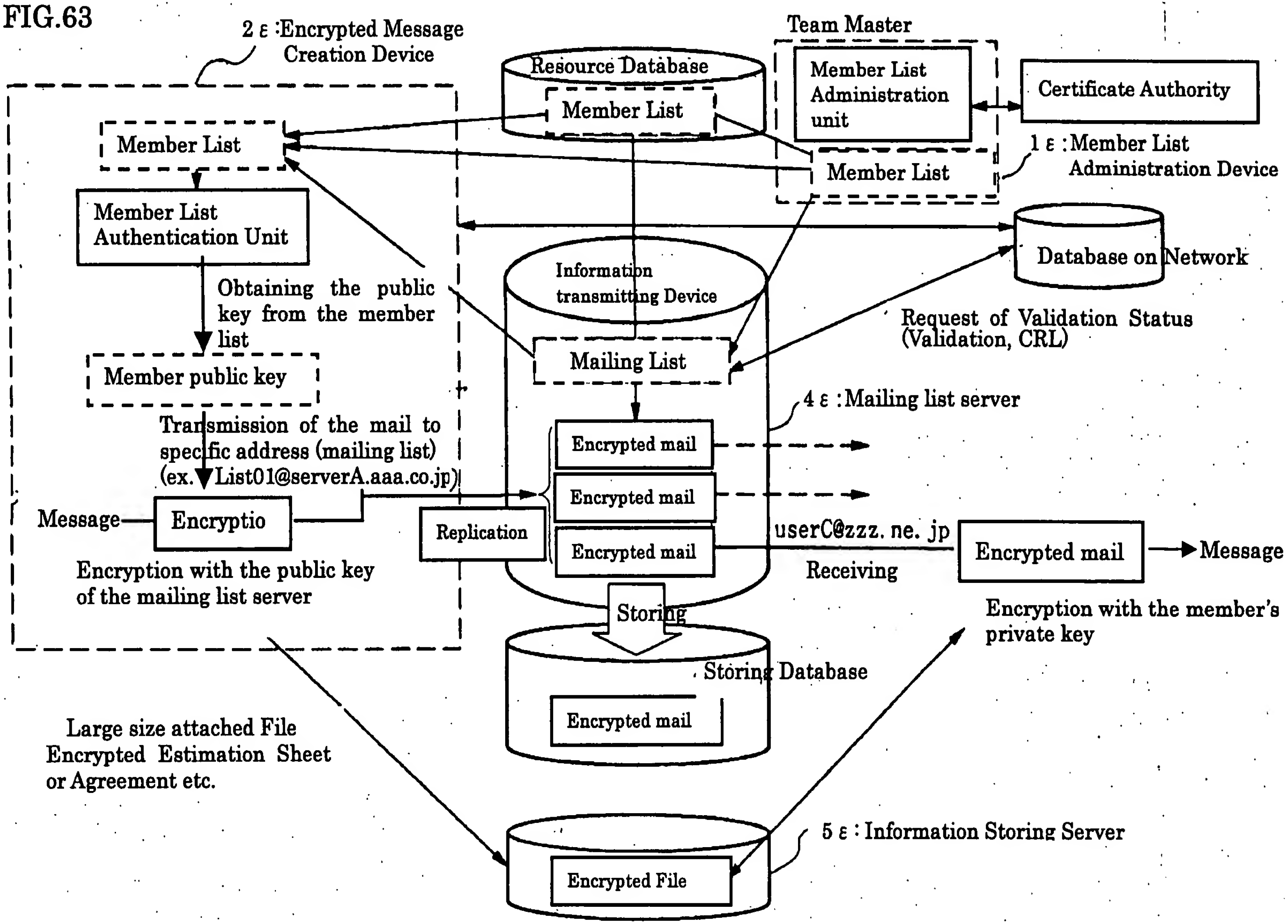

2 ε :Encrypted Message Creation Device
Member List
Member List Authentication Unit
Obtaining the public key from the member list
Member public key
Transmission of the mail to specific address (mailing list) (ex. List01@serverA.aaa.co.jp)
Message
Encryptio
Encryption with the public key of the mailing list server
Replication
Resource Database
Member List
Team Master
Member List Administration unit
Certificate Authority
Member List
1 ε :Member List Administration Device
Database on Network
Request of Validation Status (Validation, CRL)
Information transmitting Device
Mailing List
4 ε :Mailing list server
Encrypted mail
Encrypted mail
Encrypted mail
userC@zzz. ne. jp
Receiving
Encrypted mail
Message
Encryption with the member's private key
Storing
Storing Database
Encrypted mail
Large size attached File Encrypted Estimation Sheet or Agreement etc.
Encrypted File
5 ε : Information Storing Server

FIG.64

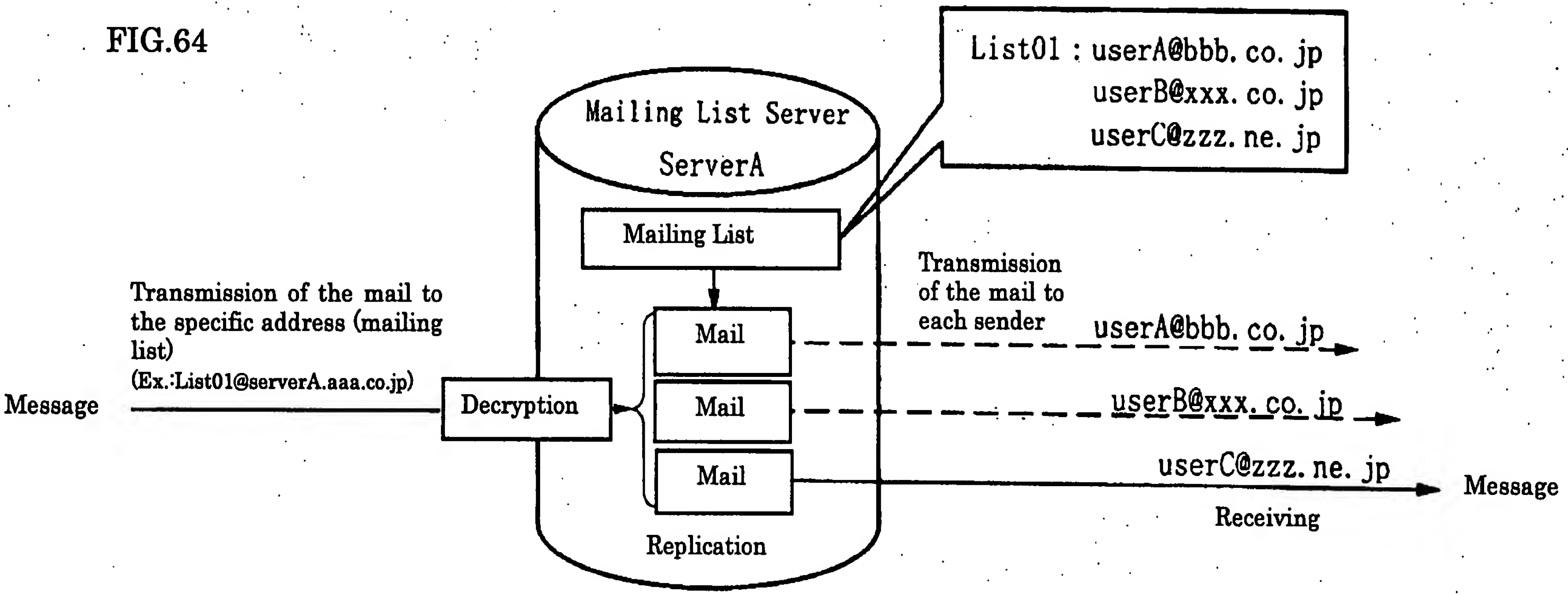

Mailing List Server
ServerA
Mailing List
List01 : userA@bbb. co. jp
userB@xxx. co. jp
userC@zzz. ne. jp
Message
Transmission of the mail to the specific address (mailing list)
(Ex.:List01@serverA.aaa.co.jp)
Decryption
Mail
Mail
Mail
Replication
Transmission of the mail to each sender
userA@bbb. co. jp
userB@xxx. co. jp
userC@zzz. ne. jp
Message
Receiving

FIG.65

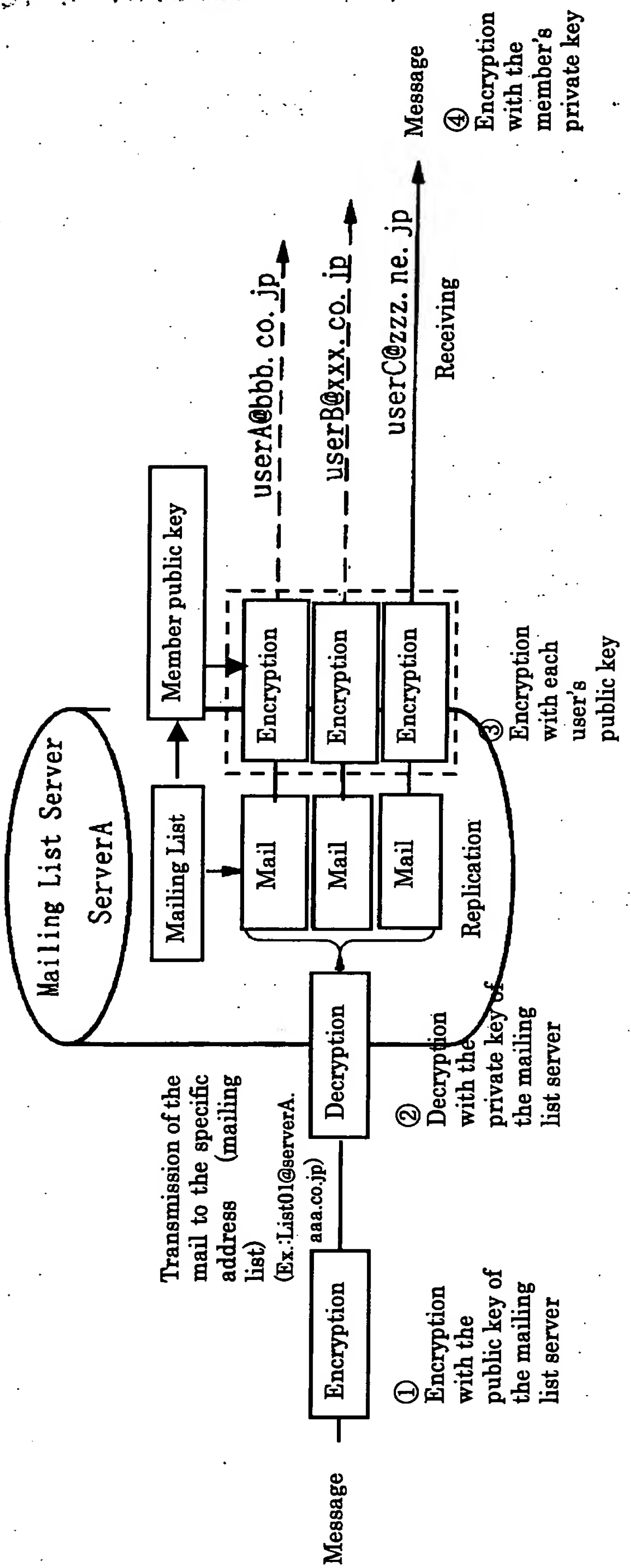

Message
① Encryption with the public key of the mailing list server
Encryption
Transmission of the mail to the specific address (mailing list)
(Ex.:List01@serverA.aaa.co.jp)
Decryption
② Decryption with the private key of the mailing list server
Mailing List Server
ServerA
Mailing List
Member public key
Mail
Mail
Mail
Replication
Encryption
Encryption
Encryption
③ Encryption with each user's public key
userA@bbb.co.jp
userB@xxx.co.jp
userC@zzz.ne.jp
Receiving
Message
④ Encryption with the member's private key

FIG.66

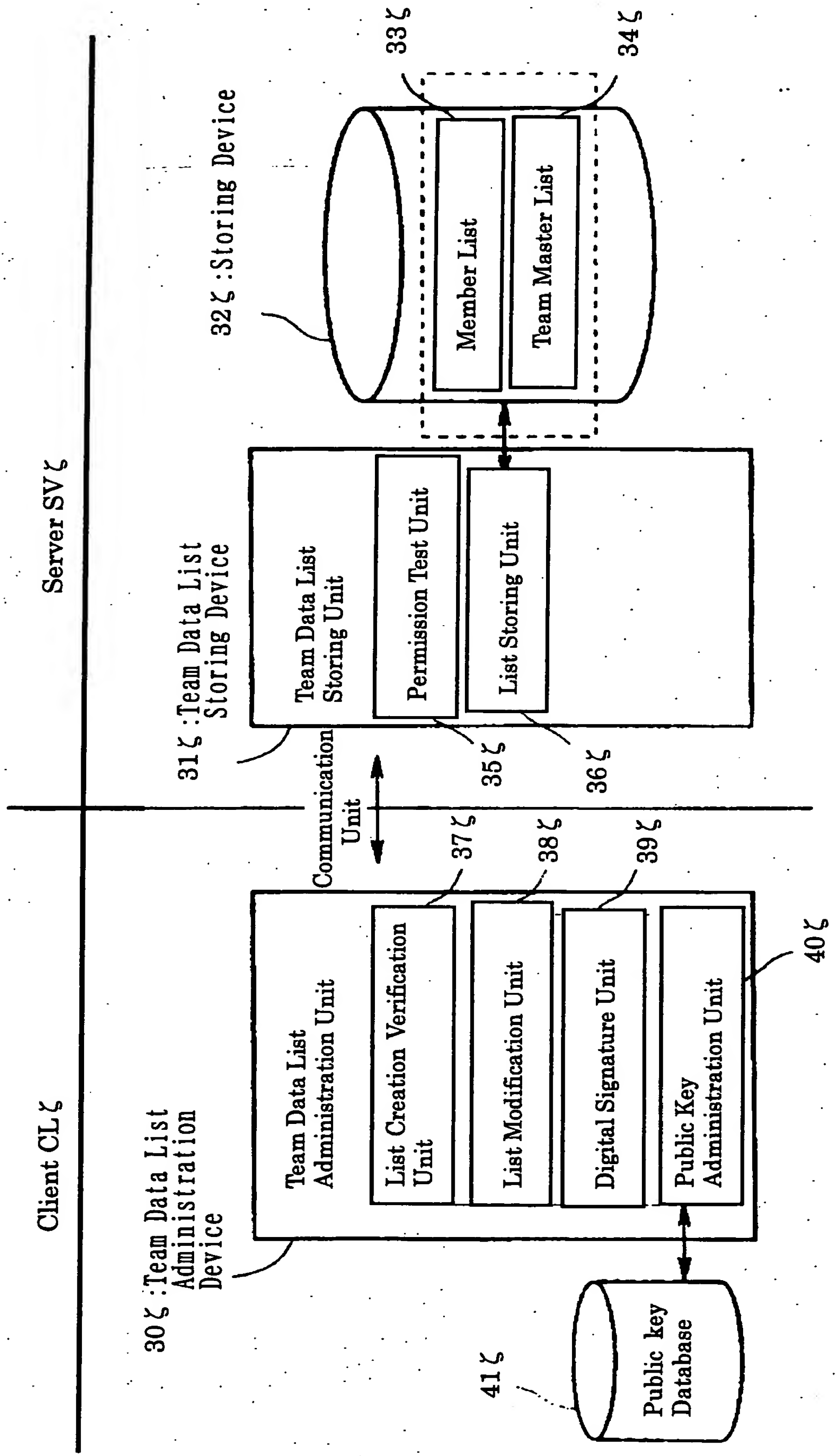

Server SV
Client CL
32 :Storing Device
33
34
Member List
Team Master List
31 :Team Data List Storing Device
Team Data List Storing Unit
Permission Test Unit
List Storing Unit
35
36
Communication Unit
30 :Team Data List Administration Device
Team Data List Administration Unit
List Creation Verification Unit
List Modification Unit
Digital Signature Unit
Public Key Administration Unit
37
38
39
40
41
Public key Database

FIG.67

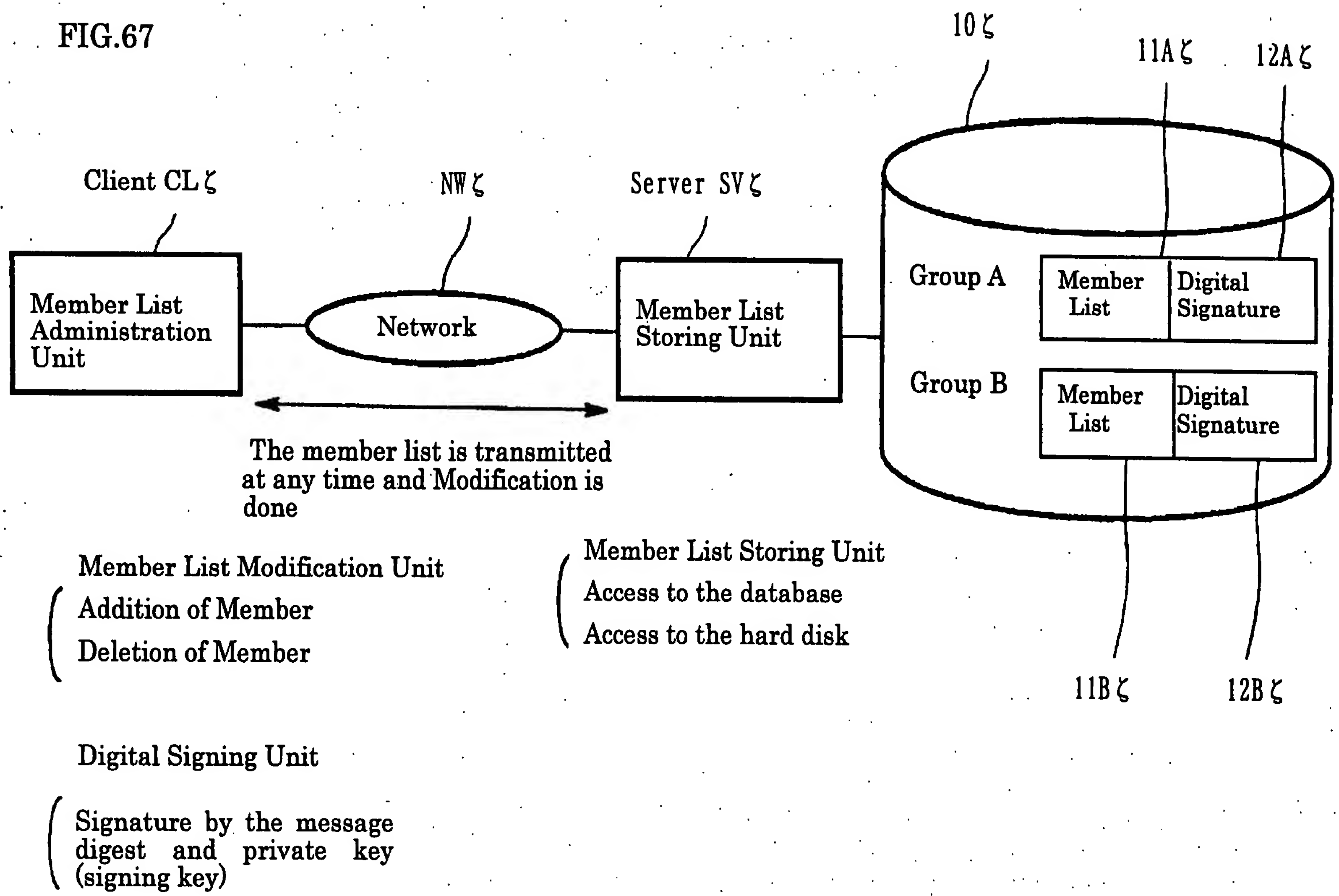

10
11A
12A
Client CL
NW
Server SV
Member List Administration Unit
Network
Member List Storing Unit
Group A
Member List
Digital Signature
Group B
Member List
Digital Signature
The member list is transmitted at any time and Modification is done
Member List Modification Unit
Addition of Member
Deletion of Member
Member List Storing Unit
Access to the database
Access to the hard disk
11B
12B
Digital Signing Unit
Signature by the message digest and private key (signing key)

FIG.68

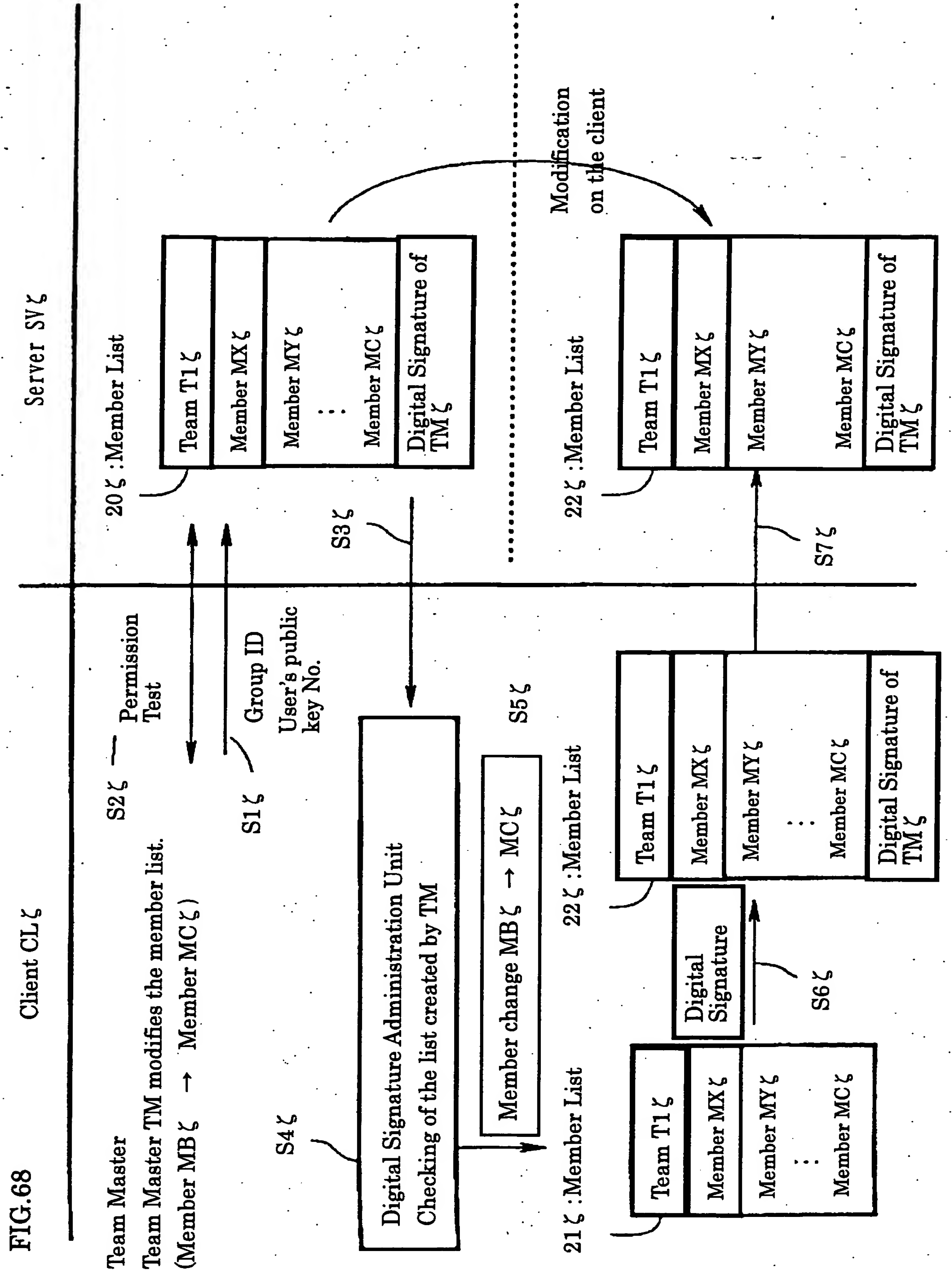

Client CLζ
Server SVζ
Team Master
Team Master TM modifies the member list.
(Member MBζ → Member MCζ)
S1ζ
Group ID
User's public key No.
S2ζ
Permission Test
20ζ :Member List
Team T1ζ
Member MXζ
Member MYζ
...
Member MCζ
Digital Signature of TMζ
S3ζ
S4ζ
Digital Signature Administration Unit
Checking of the list created by TM
S5ζ
Member change MBζ → MCζ
21ζ :Member List
Team T1ζ
Member MXζ
Member MYζ
...
Member MCζ
S6ζ
Digital Signature
22ζ :Member List
Team T1ζ
Member MXζ
Member MYζ
...
Member MCζ
Digital Signature of TMζ
S7ζ
22ζ :Member List
Team T1ζ
Member MXζ
Member MYζ
Member MCζ
Digital Signature of TMζ
Modification on the client

FIG.69

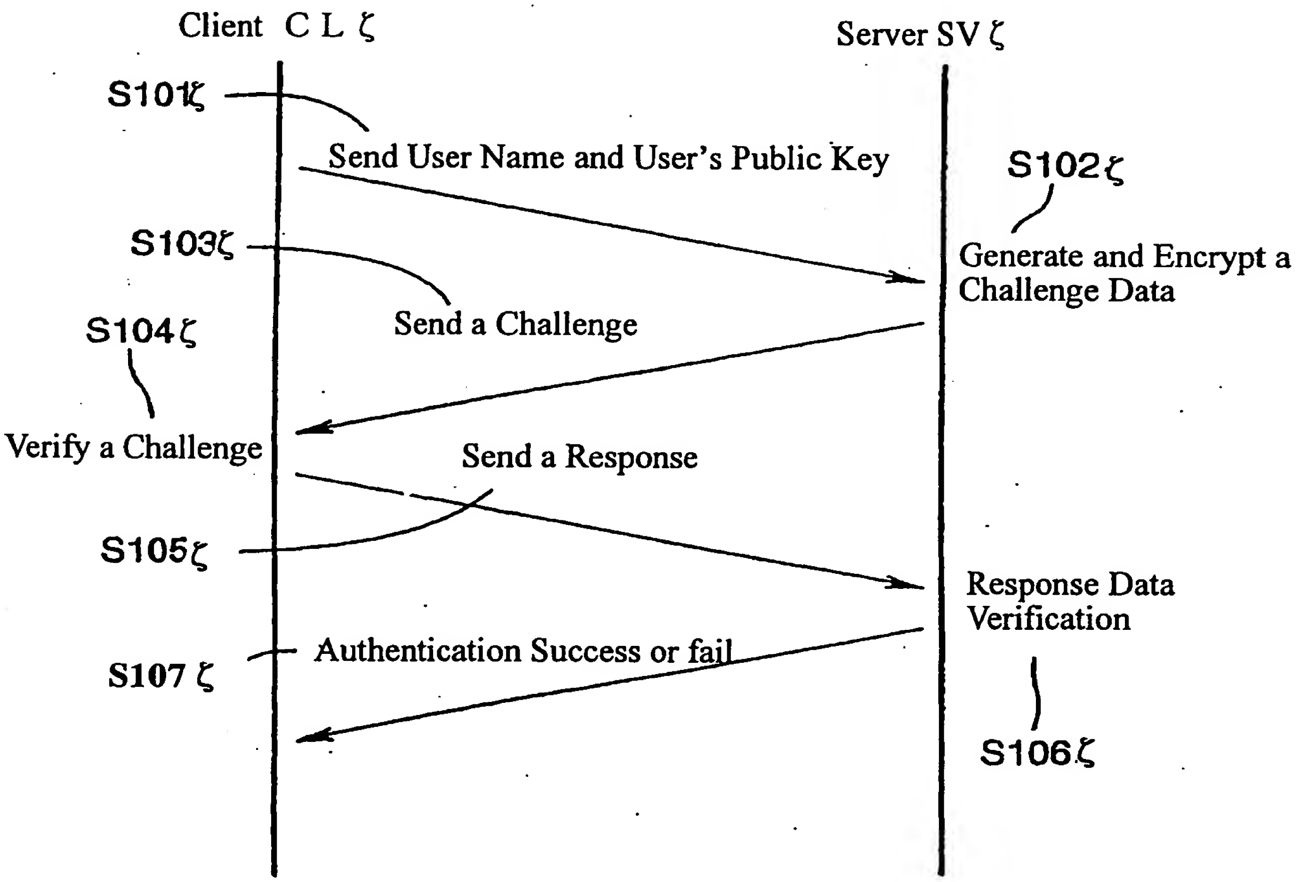

Client CL
Server SV
S101
Send User Name and User's Public Key
S102
Generate and Encrypt a Challenge Data
S103
Send a Challenge
S104
Verify a Challenge
Send a Response
S105
Response Data Verification
S107
Authentication Success or fail
S106

FIG.70

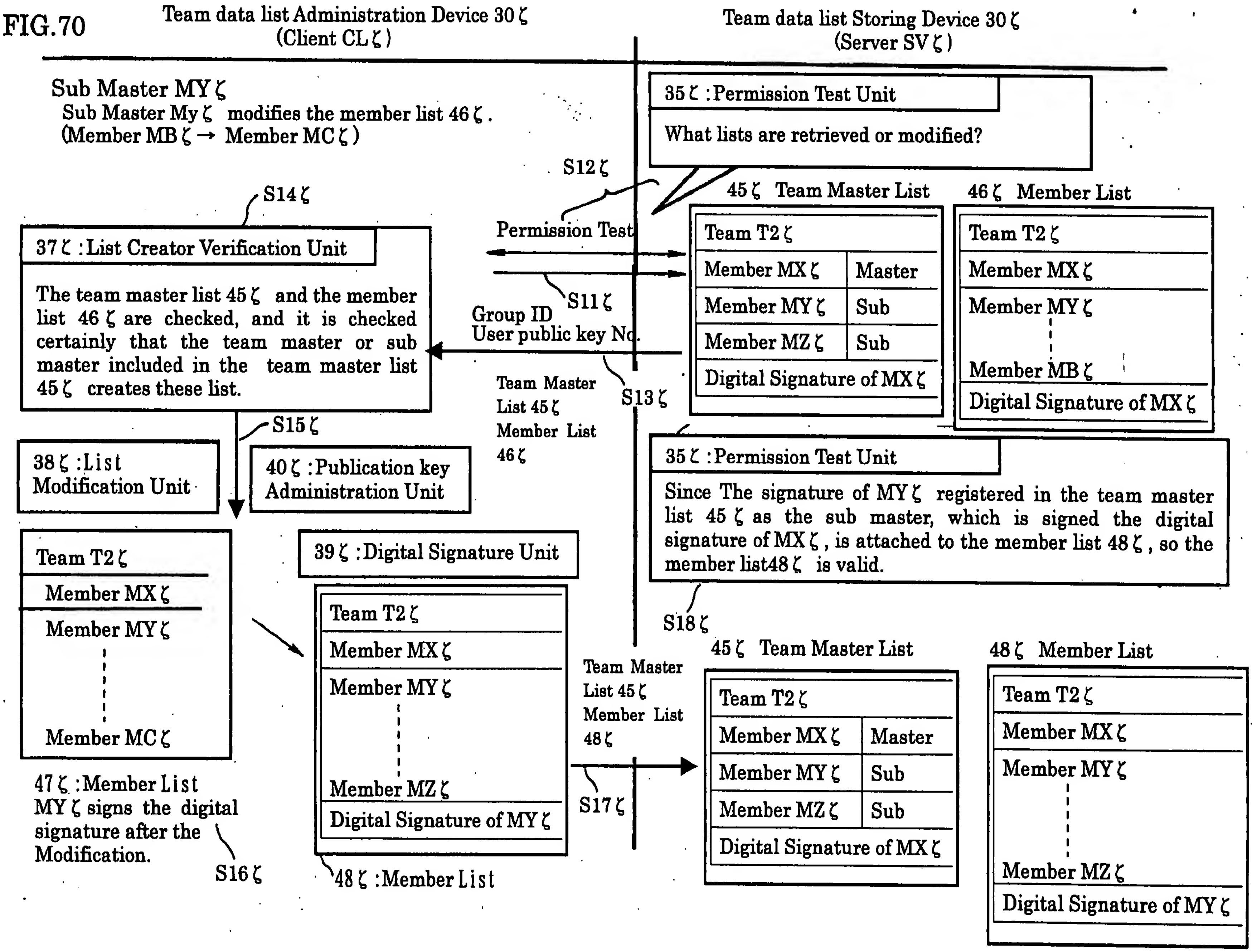

Team data list Administration Device 30ζ
(Client CLζ)
Team data list Storing Device 30ζ
(Server SVζ)
Sub Master MYζ
Sub Master Myζ modifies the member list 46ζ.
(Member MBζ → Member MCζ)
35ζ :Permission Test Unit
What lists are retrieved or modified?
S12ζ
Permission Test
S11ζ
Group ID
User public key No.
S13ζ
Team Master List 45ζ Member List 46ζ
45ζ Team Master List
Team T2ζ
Member MXζ
Master
Member MYζ
Sub
Member MZζ
Sub
Digital Signature of MXζ
46ζ Member List
Team T2ζ
Member MXζ
Member MYζ
Member MBζ
Digital Signature of MXζ
S14ζ
37ζ :List Creator Verification Unit
The team master list 45ζ and the member list 46ζ are checked, and it is checked certainly that the team master or sub master included in the team master list 45ζ creates these list.
S15ζ
38ζ :List Modification Unit
40ζ :Publication key Administration Unit
39ζ :Digital Signature Unit
Team T2ζ
Member MXζ
Member MYζ
Member MCζ
47ζ :Member List
MYζ signs the digital signature after the Modification.
S16ζ
Team T2ζ
Member MXζ
Member MYζ
Member MZζ
Digital Signature of MYζ
48ζ :Member List
Team Master List 45ζ Member List 48ζ
S17ζ
35ζ :Permission Test Unit
Since The signature of MYζ registered in the team master list 45ζ as the sub master, which is signed the digital signature of MXζ, is attached to the member list 48ζ, so the member list48ζ is valid.
S18ζ
45ζ Team Master List
Team T2ζ
Member MXζ
Master
Member MYζ
Sub
Member MZζ
Sub
Digital Signature of MXζ
48ζ Member List
Team T2ζ
Member MXζ
Member MYζ
Member MZζ
Digital Signature of MYζ

FIG. 71

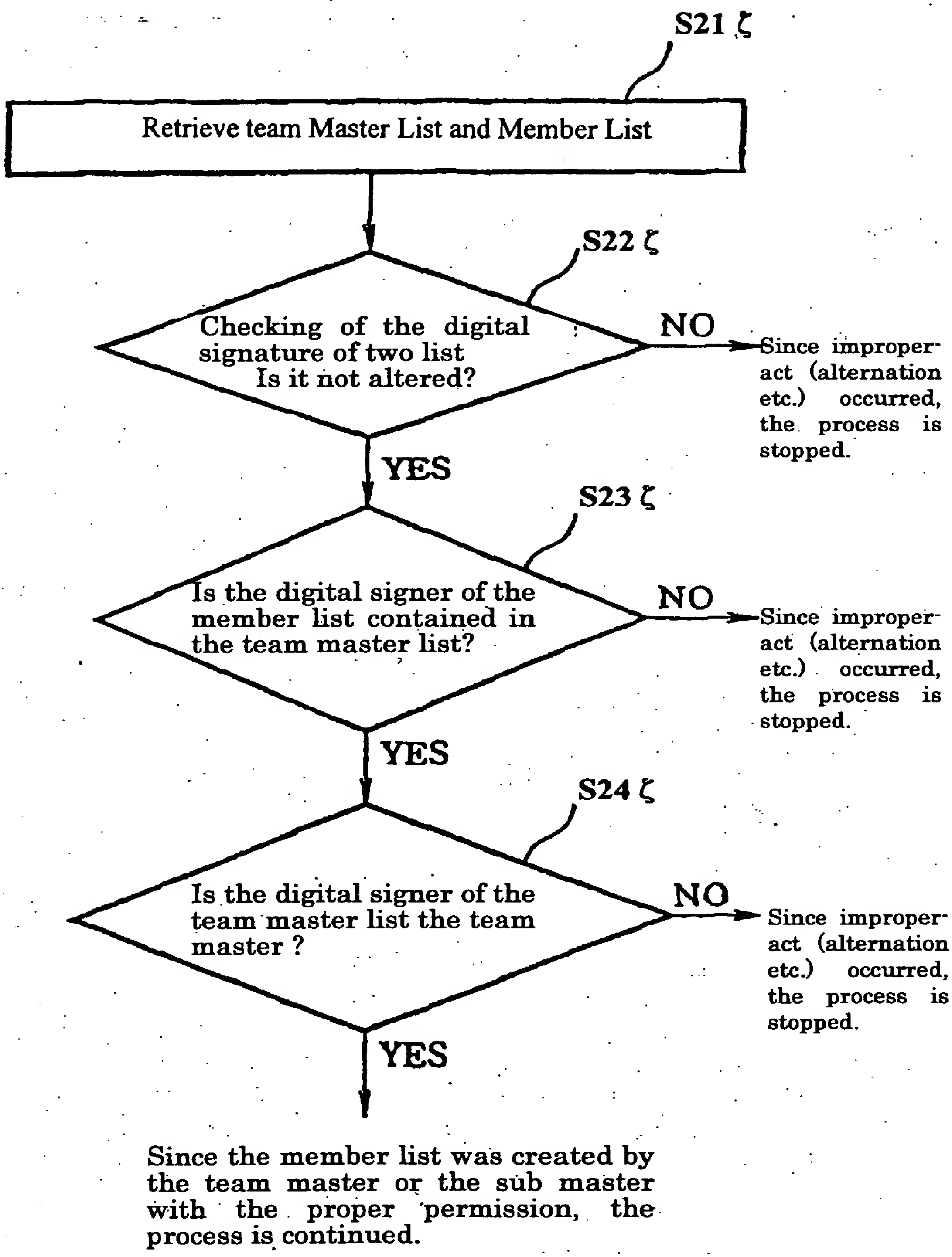

S21
Retrieve team Master List and Member List
S22
Checking of the digital signature of two list Is it not altered?
NO
Since improper-act (alternation etc.) occurred, the process is stopped.
YES
S23
Is the digital signer of the member list contained in the team master list?
NO
Since improper-act (alternation etc.) occurred, the process is stopped.
YES
S24
Is the digital signer of the team master list the team master ?
NO
Since improper-act (alternation etc.) occurred, the process is stopped.
YES
Since the member list was created by the team master or the sub master with the proper permission, the process is continued.

FIG.72

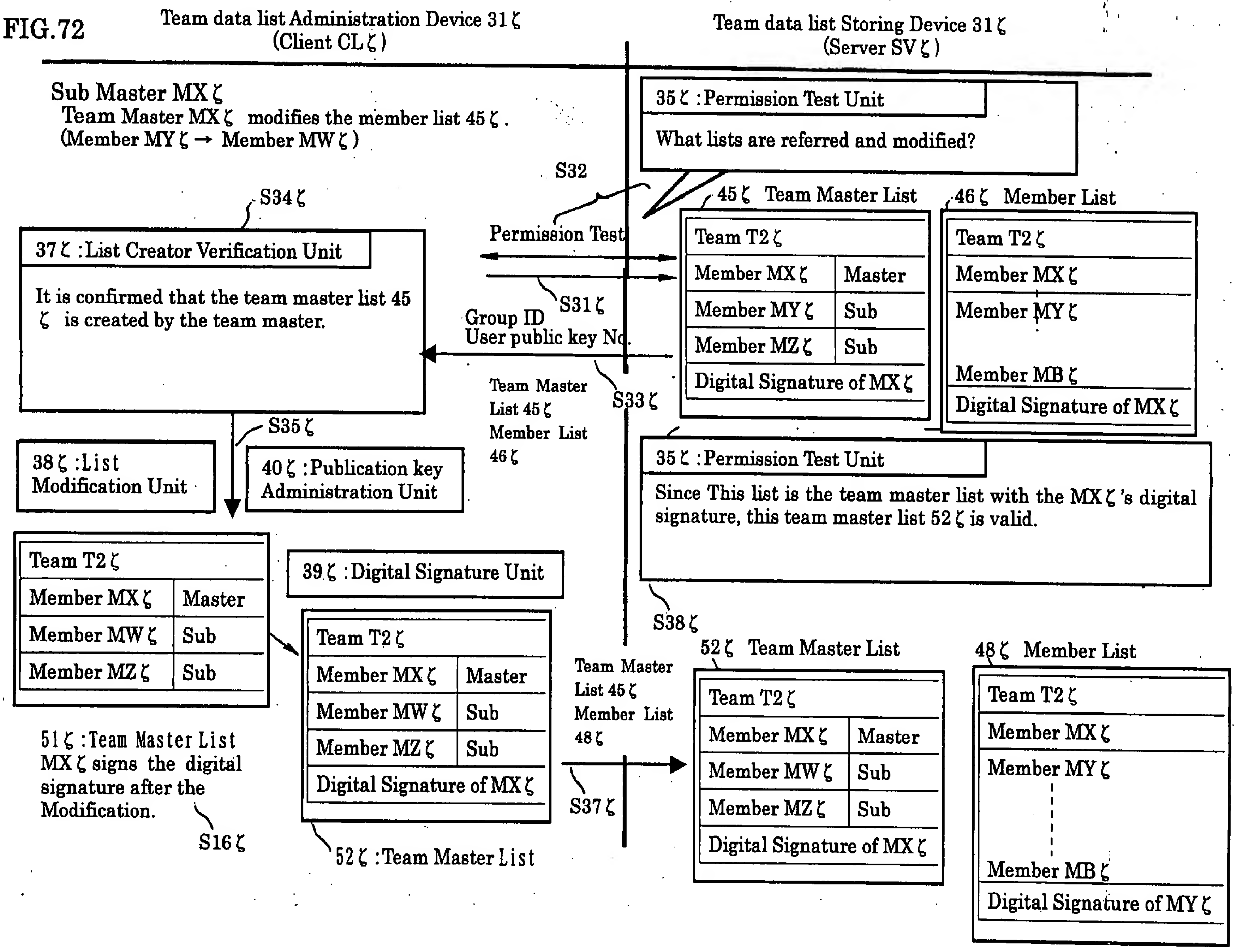

Team data list Administration Device 31ζ (Client CLζ)
Team data list Storing Device 31ζ (Server SVζ)
Sub Master MXζ
Team Master MXζ modifies the member list 45ζ.
(Member MYζ → Member MWζ)
35ζ :Permission Test Unit
What lists are referred and modified?
S32
Permission Test
S31ζ
Group ID
User public key No.
S33ζ
S34ζ
37ζ :List Creator Verification Unit
It is confirmed that the team master list 45ζ is created by the team master.
45ζ Team Master List
Team T2ζ
Member MXζ Master
Member MYζ Sub
Member MZζ Sub
Digital Signature of MXζ
46ζ Member List
Team T2ζ
Member MXζ
Member MYζ
Member MBζ
Digital Signature of MXζ
Team Master List 45ζ
Member List 46ζ
S35ζ
38ζ :List Modification Unit
40ζ :Publication key Administration Unit
35ζ :Permission Test Unit
Since This list is the team master list with the MXζ's digital signature, this team master list 52ζ is valid.
Team T2ζ
Member MXζ Master
Member MWζ Sub
Member MZζ Sub
39ζ :Digital Signature Unit
Team T2ζ
Member MXζ Master
Member MWζ Sub
Member MZζ Sub
Digital Signature of MXζ
52ζ :Team Master List
51ζ :Team Master List
MXζ signs the digital signature after the Modification.
S16ζ
S38ζ
Team Master List 45ζ
Member List 48ζ
S37ζ
52ζ Team Master List
Team T2ζ
Member MXζ Master
Member MWζ Sub
Member MZζ Sub
Digital Signature of MXζ
48ζ Member List
Team T2ζ
Member MXζ
Member MYζ
Member MBζ
Digital Signature of MYζ

FIG.73

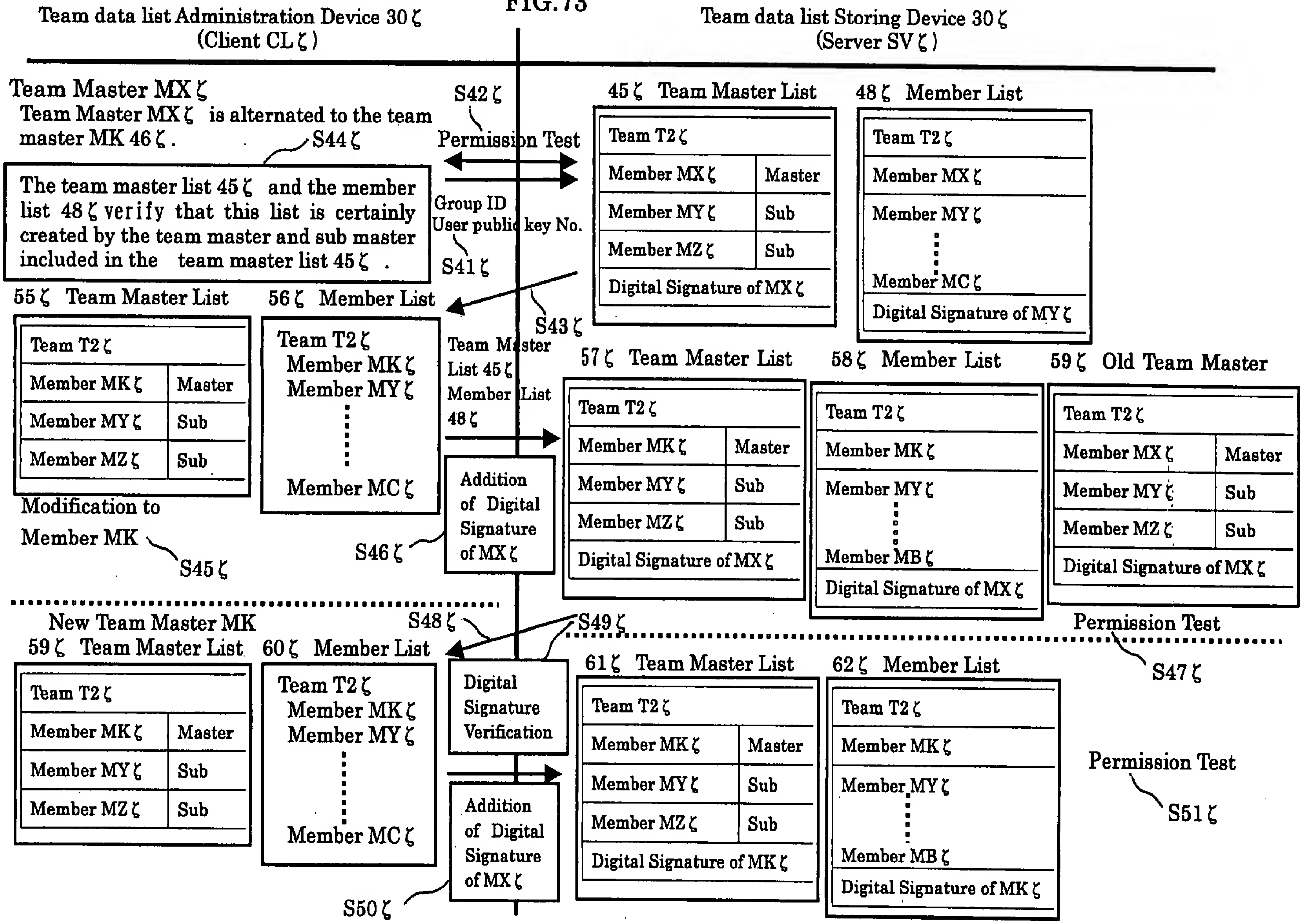

Team data list Administration Device 30ζ
(Client CLζ)
Team data list Storing Device 30ζ
(Server SVζ)
Team Master MXζ
Team Master MXζ is alternated to the team master MK 46ζ.
S44ζ
The team master list 45ζ and the member list 48ζ verify that this list is certainly created by the team master and sub master included in the team master list 45ζ .
S42ζ
Permission Test
Group ID
User public key No.
S41ζ
S43ζ
45ζ Team Master List
Team T2ζ
Member MXζ
Master
Member MYζ
Sub
Member MZζ
Sub
Digital Signature of MXζ
48ζ Member List
Team T2ζ
Member MXζ
Member MYζ
Member MCζ
Digital Signature of MYζ
55ζ Team Master List
Team T2ζ
Member MKζ
Master
Member MYζ
Sub
Member MZζ
Sub
56ζ Member List
Team T2ζ
Member MKζ
Member MYζ
Member MCζ
Modification to Member MK
S45ζ
Team Master List 45ζ
Member List 48ζ
Addition of Digital Signature of MXζ
S46ζ
57ζ Team Master List
Team T2ζ
Member MKζ
Master
Member MYζ
Sub
Member MZζ
Sub
Digital Signature of MXζ
58ζ Member List
Team T2ζ
Member MKζ
Member MYζ
Member MBζ
Digital Signature of MXζ
59ζ Old Team Master
Team T2ζ
Member MXζ
Master
Member MYζ
Sub
Member MZζ
Sub
Digital Signature of MXζ
Permission Test
S47ζ
New Team Master MK
59ζ Team Master List
Team T2ζ
Member MKζ
Master
Member MYζ
Sub
Member MZζ
Sub
60ζ Member List
Team T2ζ
Member MKζ
Member MYζ
Member MCζ
S48ζ
S49ζ
Digital Signature Verification
Addition of Digital Signature of MXζ
S50ζ
61ζ Team Master List
Team T2ζ
Member MKζ
Master
Member MYζ
Sub
Member MZζ
Sub
Digital Signature of MKζ
62ζ Member List
Team T2ζ
Member MKζ
Member MYζ
Member MBζ
Digital Signature of MKζ
Permission Test
S51ζ

FIG.74

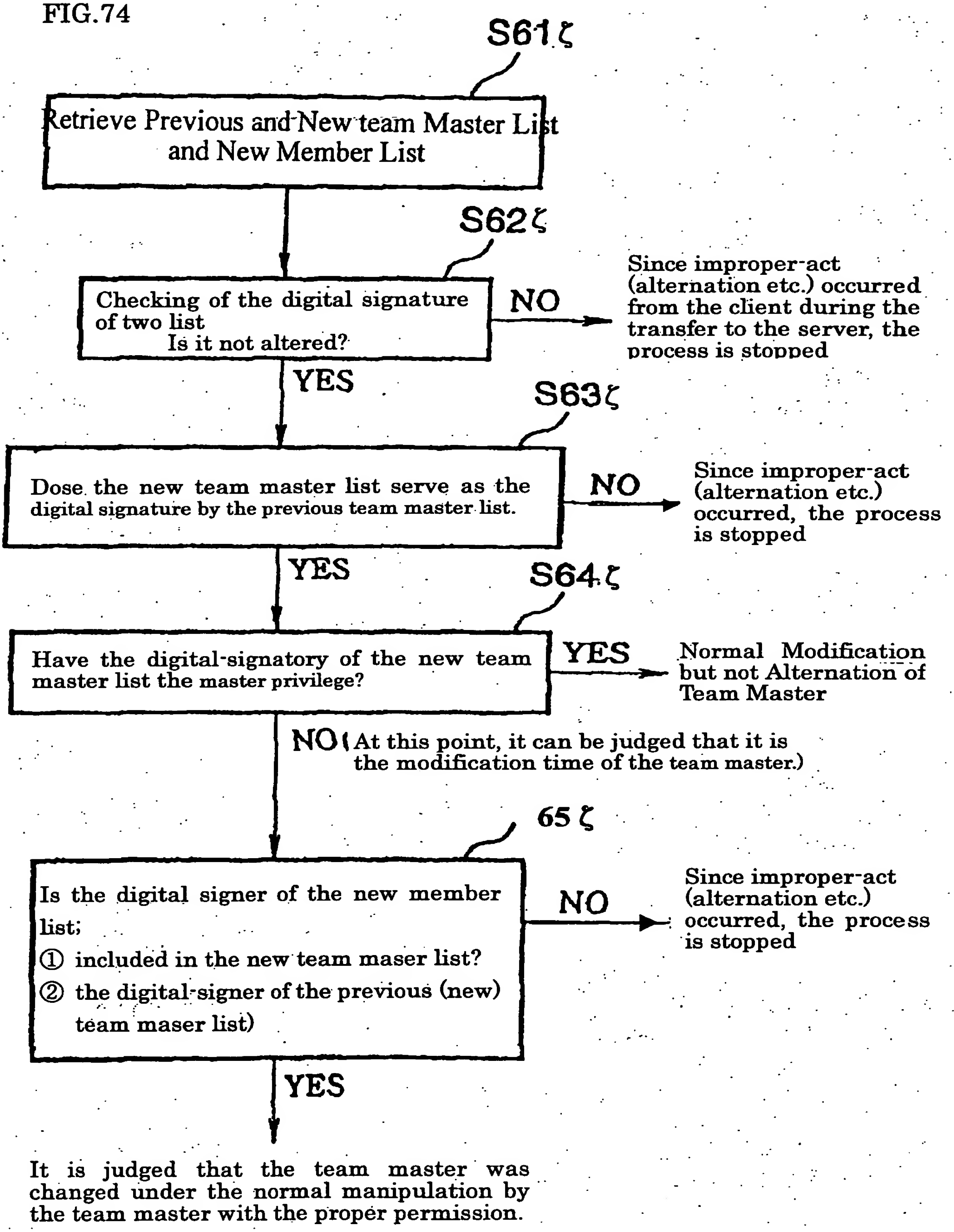

S61
Retrieve Previous and New team Master List and New Member List
S62
Checking of the digital signature of two list
Is it not altered?
NO
Since improper-act (alternation etc.) occurred from the client during the transfer to the server, the process is stopped
YES
S63
Dose the new team master list serve as the digital signature by the previous team master list.
NO
Since improper-act (alternation etc.) occurred, the process is stopped
YES
S64
Have the digital-signatory of the new team master list the master privilege?
YES
Normal Modification but not Alternation of Team Master
NO (At this point, it can be judged that it is the modification time of the team master.)
65
Is the digital signer of the new member list;
① included in the new team maser list?
② the digital-signer of the previous (new) team maser list)
NO
Since improper-act (alternation etc.) occurred, the process is stopped
YES
It is judged that the team master was changed under the normal manipulation by the team master with the proper permission.

FIG.75

The list stored at the server side

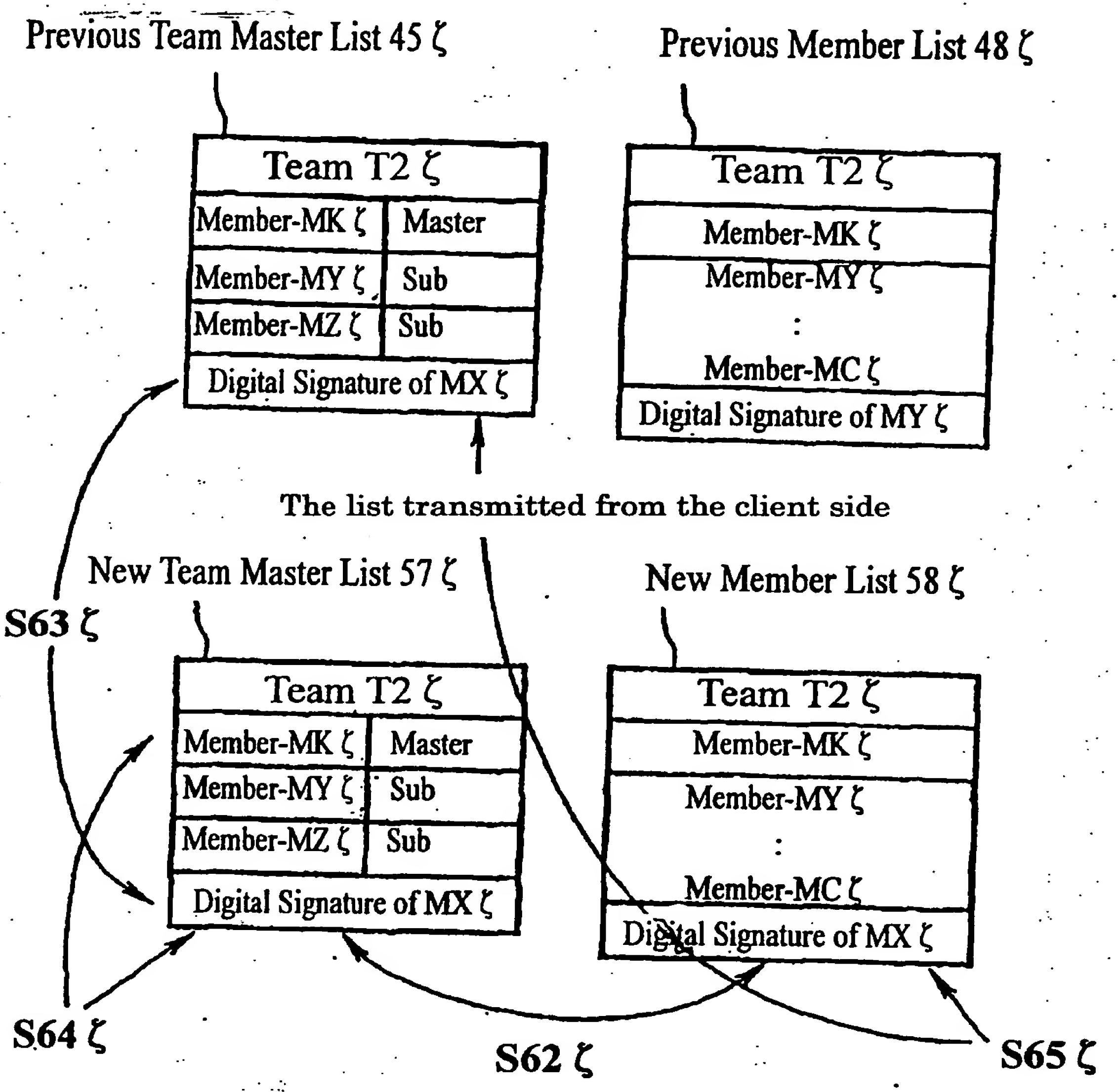


FIG.76

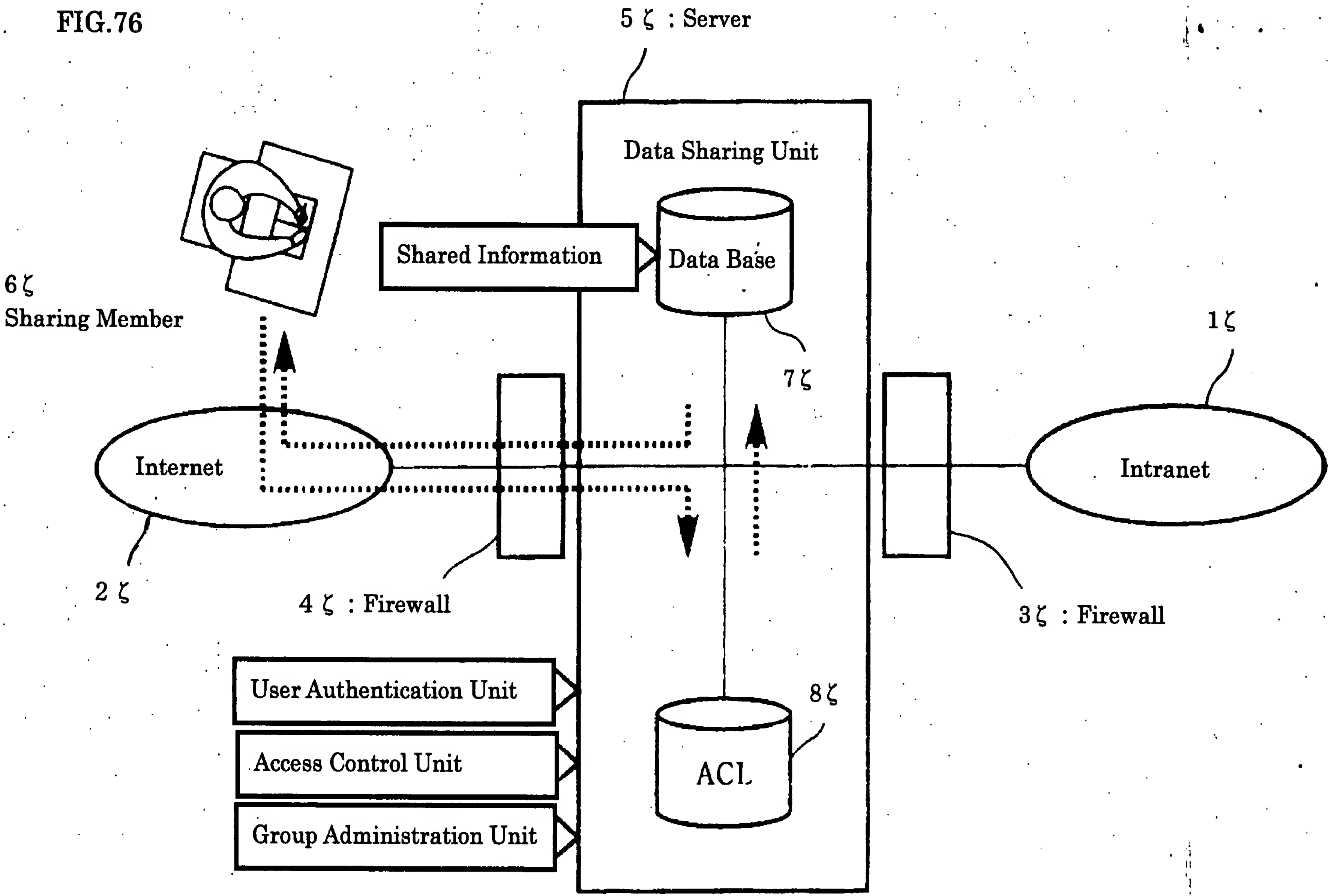
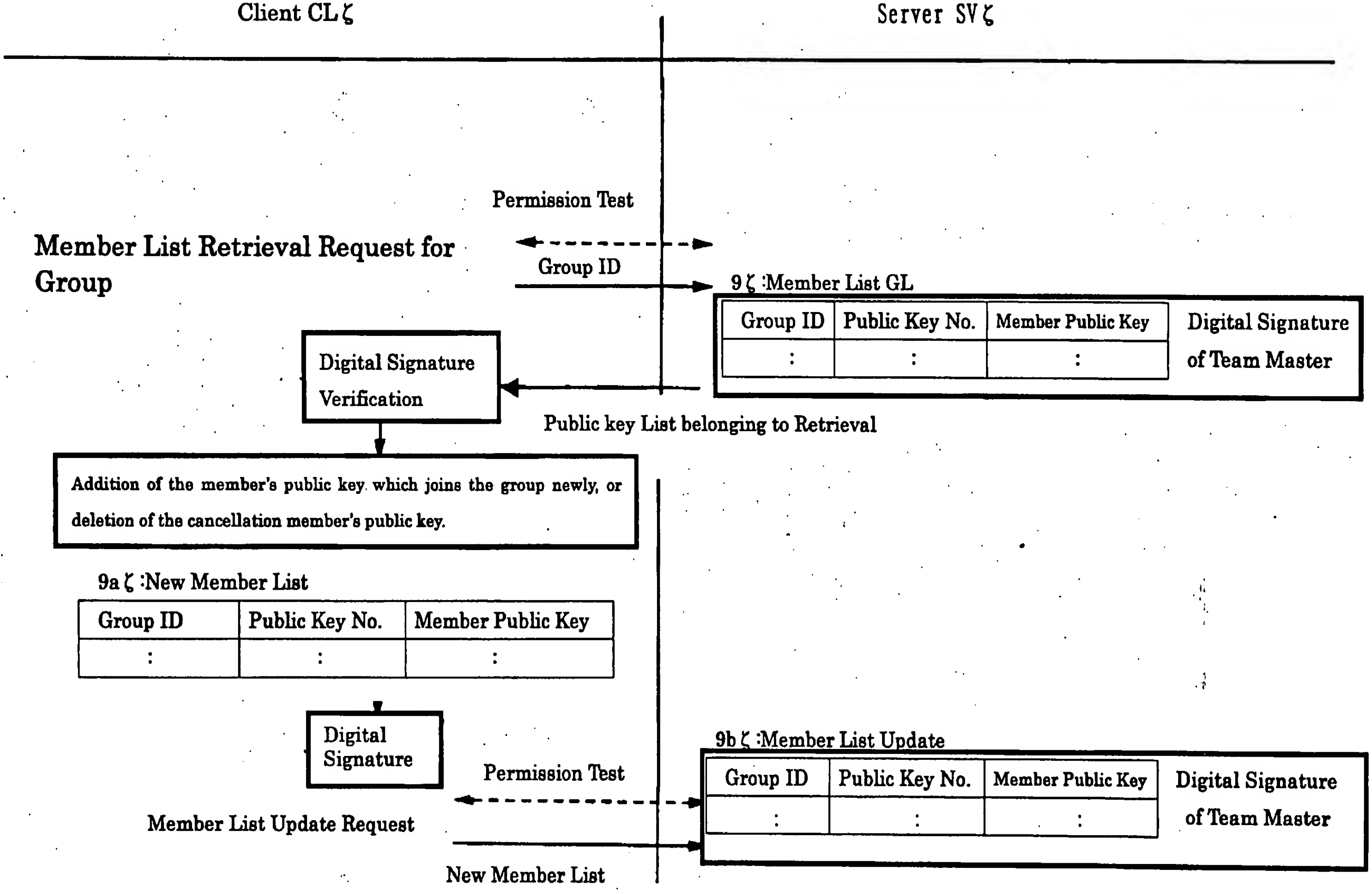

5ζ : Server
Data Sharing Unit
Shared Information
Data Base
7ζ
6ζ
Sharing Member
1ζ
Internet
Intranet
2ζ
4ζ : Firewall
3ζ : Firewall
User Authentication Unit
Access Control Unit
Group Administration Unit
8ζ
ACL

FIG.77


Client CLζ
Server SVζ
Member List Retrieval Request for Group
Permission Test
Group ID
9ζ :Member List GL
Group ID
Public Key No.
Member Public Key
:
:
:
Digital Signature of Team Master
Digital Signature Verification
Public key List belonging to Retrieval
Addition of the member's public key which joins the group newly, or deletion of the cancellation member's public key.
9aζ :New Member List
Group ID
Public Key No.
Member Public Key
:
:
:
Digital Signature
Permission Test
Member List Update Request
New Member List
9bζ :Member List Update
Group ID
Public Key No.
Member Public Key
:
:
:
Digital Signature of Team Master